



Panduan Pengguna

AWS Audit Manager



AWS Audit Manager: Panduan Pengguna

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

.....	xx
Apa itu AWS Audit Manager?	1
Fitur dari AWS Audit Manager	1
Harga untuk AWS Audit Manager	3
Apakah Anda pengguna Audit Manager pertama kali?	3
Terkait Layanan AWS	3
Lebih banyak AWS Audit Manager sumber daya	5
Konsep dan terminologi	5
A	6
C	8
D	13
E	16
F	19
I	21
R	21
D	23
Cara kerja pengumpulan bukti	24
Frekuensi pengumpulan bukti	25
Contoh kontrol	26
Kontrol otomatis (Security Hub CSPM)	28
Kontrol otomatis (AWS Config)	29
Kontrol otomatis (panggilan API)	31
Kontrol otomatis (CloudTrail)	33
Kontrol manual	36
Kontrol dengan sumber data campuran	37
Penggunaan AWS Audit Manager	40
Menggunakan Audit Manager dengan AWS SDK	41
Menggunakan Audit Manager dengan CloudFormation	42
Third-party Integrasi GRC	43
Mengintegrasikan bukti Audit Manager ke dalam sistem GRC Anda	46
AWS Audit Manager perubahan ketersediaan	59
Batasan Paket Kesesuaian untuk pelanggan Audit Manager	59
AWS Audit Manager Kerangka Pemetaan ke AWS Config Paket Kesesuaian	60
Mengekspor bukti dari AWS Config	62

Membandingkan solusi kepatuhan	64
Menonaktifkan AWS Audit Manager	65
Sumber daya tambahan	66
Pertanyaan yang Sering Diajukan	66
Kerangka kerja yang didukung	70
ACSC Essential Delapan	71
Apa itu Delapan Esensi?	72
Menggunakan Framework ini	72
Langkah selanjutnya	73
Sumber daya tambahan	74
ACSC ISME	74
Apa itu ACSC ISM?	74
Menggunakan Framework ini	74
Langkah selanjutnya	76
Sumber daya tambahan	76
AWS Audit Manager Contoh Kerangka	76
Apa kerangka AWS Audit Manager sampel?	77
Menggunakan Framework ini	77
Langkah selanjutnya	78
AWS Control Tower Pagar pembatas	78
Apa itu AWS Control Tower?	79
Menggunakan Framework ini	79
Langkah selanjutnya	80
Sumber daya tambahan	81
AWS Praktik Terbaik AI Generatif	81
Apa praktik terbaik AI AWS generatif untuk Amazon Bedrock?	82
Menggunakan Framework ini	84
Memverifikasi petunjuk secara manual di Amazon Bedrock	86
Langkah selanjutnya	89
Sumber daya tambahan	89
AWS License Manager	89
Apa itu AWS License Manager?	90
Menggunakan Framework ini	90
Langkah selanjutnya	91
Sumber daya tambahan	91
AWS Praktik Terbaik Keamanan Dasar	92

Apa standar Praktik Terbaik Keamanan AWS Dasar?	92
Menggunakan Framework ini	92
Langkah selanjutnya	93
Sumber daya tambahan	94
AWS Praktik Terbaik Operasional	94
Apa standar Praktik Terbaik Keamanan AWS Dasar?	94
Menggunakan Framework ini	95
Langkah selanjutnya	96
Sumber daya tambahan	96
AWS Kerangka Kerja yang Diarsiteksikan dengan Baik WAF v10	96
Apa itu Kerangka AWS Well-Architected?	96
Menggunakan Framework ini	97
Langkah selanjutnya	98
Sumber daya tambahan	94
Profil Kontrol Awan Menengah CCCS	98
Apa itu CCCS?	99
Menggunakan Framework ini	99
Langkah selanjutnya	101
AWS Tolok Ukur CIS v.1.2	101
Apa itu CIS?	101
Menggunakan Framework ini	102
Langkah selanjutnya	111
Sumber daya tambahan	111
AWS Tolok Ukur CIS v.1.3	111
Apa itu Tolok Ukur AWS CIS?	112
Menggunakan kerangka kerja ini	113
Langkah selanjutnya	114
Sumber daya tambahan	115
AWS Tolok Ukur CIS v.1.4	115
Apa itu AWS Tolok Ukur CIS?	115
Menggunakan kerangka kerja ini	117
Langkah selanjutnya	118
Sumber daya tambahan	118
Kontrol CIS v7.1 IG1	118
Apa itu Kontrol CIS?	119
Menggunakan Framework ini	120

Langkah selanjutnya	121
Sumber daya tambahan	121
Kontrol Keamanan Kritis CIS versi 8.0, IG1	121
Apa itu Kontrol CIS?	122
Menggunakan Framework ini	123
Langkah selanjutnya	124
Sumber daya tambahan	124
Kontrol Dasar Keamanan FedRAMP r4	124
Apa itu FedRAMP?	125
Menggunakan Framework ini	125
Langkah selanjutnya	126
Sumber daya tambahan	126
GDPR 2016	126
Apa itu GDPR?	127
Menggunakan Framework ini	127
Langkah selanjutnya	152
Sumber daya tambahan	152
GLBA	152
Apa itu GLBA?	153
Menggunakan Framework ini	153
Langkah selanjutnya	154
Judul 21 CFR Bagian 11	154
Apa Judul 21 dari CFR Bagian 11?	155
Menggunakan Framework ini	155
Langkah selanjutnya	156
Sumber daya tambahan	156
Lampiran GMP UE 11, v1	157
Apa itu EU GMP Annex 11?	157
Menggunakan Framework ini	157
Langkah selanjutnya	159
Aturan Keamanan HIPAA: Feb 2003	159
Apa itu HIPAA dan Aturan Keamanan HIPAA 2003?	159
Menggunakan Framework ini	160
Langkah selanjutnya	162
Sumber daya tambahan	162
Aturan Akhir Omnibus HIPAA	162

Apa itu HIPAA dan Aturan Keamanan Omnibus Akhir HIPAA?	163
Menggunakan Framework ini	160
Langkah selanjutnya	165
Sumber daya tambahan	165
ISO/IEC 27001:2013	165
Apa itu ISO/IEC 27001?	166
Menggunakan Framework ini	166
Langkah selanjutnya	167
Sumber daya tambahan	168
NIST SP 800-53 R5	168
Apa itu NIST SP 800-53?	168
Menggunakan Framework ini	169
Langkah selanjutnya	170
Sumber daya tambahan	170
NIST CSF v1.1	171
Apa itu Kerangka Keamanan Siber NIST?	171
Menggunakan Framework ini	172
Langkah selanjutnya	173
Sumber daya tambahan	173
NIST SP 800-171 R2	173
Apa itu NIST SP 800-171?	174
Menggunakan Framework ini	175
Langkah selanjutnya	176
Sumber daya tambahan	176
PCI DSS v3.2.1	176
Apa itu PCI DSS?	177
Menggunakan Framework ini	177
Langkah selanjutnya	178
Sumber daya tambahan	179
PCI DSS v4	179
Apa itu PCI DSS?	179
Menggunakan Framework ini	180
Langkah selanjutnya	182
Sumber daya tambahan	182
SSAE-18 SOC 2	182
Apa itu SOC 2?	183

Menggunakan Framework ini	183
Langkah selanjutnya	184
Sumber daya tambahan	185
Sumber data yang didukung	186
Poin kunci	186
Langkah selanjutnya	190
AWS Config	190
Poin kunci	190
Didukung AWS Config aturan yang dikelola	191
Menggunakan aturan khusus dengan Audit Manager	203
Sumber daya tambahan	203
AWS Security Hub CSPM	204
Poin kunci	204
Kontrol CSPM Security Hub yang didukung	216
Sumber daya tambahan	241
AWS Panggilan API	242
Poin kunci	242
Panggilan API yang didukung untuk sumber data kontrol kustom	243
AWS License Manager Panggilan API	254
Sumber daya tambahan	255
AWS CloudTrail	255
Sumber daya tambahan	256
Penyiapan	257
Prasyarat	257
Mendaftar untuk Akun AWS	258
Tambahkan izin yang diperlukan	258
Langkah selanjutnya	259
Mengaktifkan Manajer Audit	259
Prasyarat	259
Prosedur	259
Langkah selanjutnya	263
Rekomendasi	263
Poin kunci	264
Fitur yang disarankan	264
Integrasi yang direkomendasikan	264
Langkah selanjutnya	270

Memulai	271
Tutorial Manajer Audit	271
Tutorial untuk Pemilik Audit: Membuat penilaian	272
Prasyarat	272
Prosedur	273
Sumber daya tambahan	275
Tutorial untuk Delegasi: Meninjau kumpulan kontrol	276
Prasyarat	276
Prosedur	276
Sumber daya tambahan	281
Menggunakan dasbor	282
Konsep dan terminologi dasbor	283
Elemen dasbor	285
Filter penilaian	285
Cuplikan harian	285
Kontrol dengan bukti yang tidak sesuai dikelompokkan berdasarkan domain kontrol	286
Langkah selanjutnya	289
Sumber daya tambahan	289
Penilaian	290
Poin kunci	290
Sumber daya tambahan	290
Membuat penilaian	291
Prasyarat	292
Prosedur	292
Langkah selanjutnya	297
Sumber daya tambahan	297
Menemukan penilaian	297
Prasyarat	298
Prosedur	298
Langkah selanjutnya	299
Sumber daya tambahan	299
Meninjau penilaian	299
Poin kunci	299
Sumber daya tambahan	300
Rincian penilaian	300
Rincian kontrol penilaian	307

Rincian folder bukti	313
Rincian bukti	318
Mengedit penilaian	322
Prasyarat	322
Prosedur	323
Langkah selanjutnya	325
Sumber daya tambahan	326
Menambahkan bukti manual	326
Poin kunci	327
Sumber daya tambahan	327
Mengimpor bukti dari S3	327
Mengunggah bukti dari browser	331
Memasukkan teks sebagai bukti	336
Format file yang didukung	340
Mempersiapkan laporan penilaian	340
Poin kunci	341
Sumber daya tambahan	341
Menambahkan bukti ke laporan penilaian	341
Menghapus bukti dari laporan penilaian	343
Menghasilkan laporan penilaian	344
Mengubah status kontrol penilaian	346
Prasyarat	346
Prosedur	346
Langkah selanjutnya	348
Mengubah status penilaian	349
Prasyarat	349
Prosedur	349
Langkah selanjutnya	351
Menghapus penilaian	351
Prasyarat	352
Prosedur	352
Sumber daya tambahan	353
Delegasi	354
Poin kunci	354
Sumber daya tambahan	354
Untuk pemilik audit	355

Poin kunci	355
Sumber daya tambahan	355
Mendelegasikan set kontrol	356
Menemukan delegasi	358
Menghapus delegasi	360
Untuk delegasi	361
Poin kunci	361
Sumber daya tambahan	362
Melihat notifikasi	362
Meninjau kontrol dan bukti	363
Menambahkan komentar	365
Menandai kontrol sebagai ditinjau	366
Mengirimkan set kontrol ke pemilik audit	367
Laporan penilaian	369
Memahami struktur folder	369
Menavigasi laporan penilaian	370
Meninjau bagian laporan penilaian	371
Halaman sampul	371
Halaman Ikhtisar	371
Halaman daftar isi	373
Halaman kontrol	373
Halaman ringkasan bukti	375
Halaman detail bukti	376
Memvalidasi laporan penilaian	377
Sumber daya tambahan	377
Pencari bukti	378
Poin kunci	378
Memahami cara kerja pencari bukti dengan CloudTrail Lake	378
Langkah selanjutnya	379
Sumber daya tambahan	379
Mencari bukti	379
Prasyarat	380
Prosedur	380
Langkah selanjutnya	384
Sumber daya tambahan	384
Melihat hasil pencarian Anda	384

Prasyarat	385
Prosedur	385
Langkah selanjutnya	388
Sumber daya tambahan	388
Mengekspor hasil pencarian Anda	388
Prasyarat	389
Prosedur	389
Sumber daya tambahan	393
Opsi filter dan pengelompokan	393
Referensi filter	393
Referensi pengelompokan	398
Contoh kasus penggunaan	399
Kasus penggunaan 1: Temukan bukti yang tidak sesuai dan atur delegasi	399
Kasus penggunaan 2: Identifikasi bukti yang sesuai	400
Kasus penggunaan 3: Lakukan pratinjau cepat sumber bukti	401
Pusat unduhan	403
Menjelajahi pusat unduhan	403
Mengunduh file	405
Menghapus file	405
Sumber daya tambahan	406
Perpustakaan kerangka kerja	407
Poin kunci	407
Sumber daya tambahan	408
Menemukan kerangka kerja	408
Prasyarat	408
Prosedur	409
Langkah selanjutnya	410
Sumber daya tambahan	410
Meninjau kerangka kerja	410
Prasyarat	410
Prosedur	410
Langkah selanjutnya	414
Sumber daya tambahan	414
Membuat kerangka kerja khusus	414
Poin kunci	415
Sumber daya tambahan	415

Membuat dari awal	415
Membuat salinan yang dapat diedit	418
Mengedit kerangka kerja khusus	421
Prasyarat	421
Prosedur	421
Langkah selanjutnya	423
Sumber daya tambahan	423
Berbagi kerangka kerja khusus	423
Poin kunci	424
Sumber daya tambahan	424
Konsep dan terminologi	424
Mengirim permintaan berbagi	432
Menanggapi permintaan berbagi	438
Menghapus permintaan berbagi	443
Menghapus kerangka kerja khusus	444
Prasyarat	444
Prosedur	444
Sumber daya tambahan	446
Pustaka kontrol	447
Poin kunci	447
Sumber daya tambahan	447
Menemukan kontrol	448
Prasyarat	448
Prosedur	449
Langkah selanjutnya	450
Sumber daya tambahan	450
Meninjau kontrol	450
Kontrol umum	451
Kontrol inti	454
Kontrol standar	458
Kontrol kustom	463
Membuat kontrol khusus	467
Poin kunci	468
Sumber daya tambahan	469
Membuat dari awal	469
Membuat salinan yang dapat diedit	475

Mengedit kontrol khusus	480
Prasyarat	480
Prosedur	481
Langkah selanjutnya	485
Sumber daya tambahan	485
Mengubah frekuensi pengumpulan bukti	485
Menghapus kontrol khusus	489
Prasyarat	489
Prosedur	489
Sumber daya tambahan	491
Pengaturan	492
Prosedur	492
Langkah selanjutnya	492
Mengkonfigurasi pengaturan enkripsi data Anda	493
Prasyarat	493
Prosedur	494
Sumber daya tambahan	495
Menambahkan administrator yang didelegasikan	495
Prasyarat	495
Prosedur	496
Langkah selanjutnya	497
Sumber daya tambahan	497
Mengubah administrator yang didelegasikan	497
Prasyarat	498
Prosedur	499
Langkah selanjutnya	501
Sumber daya tambahan	501
Menghapus administrator yang didelegasikan	501
Prasyarat	502
Prosedur	503
Sumber daya tambahan	504
Mengkonfigurasi pemilik audit default Anda	504
Prosedur	504
Sumber daya tambahan	505
Mengkonfigurasi tujuan laporan penilaian default	506
Prasyarat	506

Prosedur	510
Sumber daya tambahan	511
Mengkonfigurasi notifikasi Audit Manager	511
Prasyarat	511
Prosedur	511
Sumber daya tambahan	512
Mengaktifkan pencari bukti	512
Prasyarat	513
Prosedur	513
Langkah selanjutnya	514
Sumber daya tambahan	514
Mengkonfirmasi status pencari bukti	514
Prasyarat	515
Prosedur	515
Langkah selanjutnya	518
Sumber daya tambahan	518
Menonaktifkan pencari bukti	518
Prasyarat	518
Prosedur	519
Sumber daya tambahan	520
Mengkonfigurasi tujuan ekspor default	520
Prasyarat	520
Prosedur	522
Notifikasi	524
Sumber daya tambahan	524
Pemecahan masalah	525
Penilaian pemecahan masalah dan pengumpulan bukti	525
Saya membuat penilaian tetapi saya belum dapat melihat bukti	526
Penilaian saya tidak mengumpulkan bukti pemeriksaan kepatuhan dari AWS Security Hub CSPM	527
Saya menonaktifkan kontrol keamanan di Security Hub CSPM. Apakah Audit Manager mengumpulkan bukti pemeriksaan kepatuhan untuk kontrol keamanan itu?	528
Saya mengatur status temuan ke Suppressed di Security Hub CSPM. Apakah Manajer Audit mengumpulkan bukti pemeriksaan kepatuhan tentang temuan itu?	529
Penilaian saya tidak mengumpulkan bukti pemeriksaan kepatuhan dari AWS Config	529
Penilaian saya tidak mengumpulkan bukti aktivitas pengguna dari AWS CloudTrail	531

Penilaian saya tidak mengumpulkan bukti data konfigurasi untuk AWS Panggilan API	532
Kontrol umum tidak mengumpulkan bukti otomatis	532
Bukti saya dihasilkan pada interval yang berbeda, dan saya tidak yakin seberapa sering itu dikumpulkan	533
Saya menonaktifkan dan kemudian mengaktifkan kembali Manajer Audit, dan sekarang penilaian saya yang sudah ada sebelumnya tidak lagi mengumpulkan bukti	535
Di halaman detail penilaian saya, saya diminta untuk membuat ulang penilaian saya	535
Apa perbedaan antara sumber data dan sumber bukti?	536
Pembuatan penilaian saya gagal	536
Apa yang terjadi jika saya menghapus akun dalam lingkup dari organisasi saya?	537
Saya tidak dapat melihat layanan dalam lingkup penilaian saya	537
Saya tidak dapat mengedit layanan dalam lingkup penilaian saya	538
Apa perbedaan antara layanan dalam ruang lingkup dan tipe sumber data?	538
Laporan penilaian pemecahan masalah	540
Laporan penilaian saya gagal menghasilkan	540
Saya mengikuti daftar periksa di atas, dan laporan penilaian saya masih gagal menghasilkan	542
Saya mendapatkan akses ditolak kesalahan saat saya mencoba membuat laporan	542
Saya tidak dapat membuka zip laporan penilaian	543
Ketika saya memilih nama bukti dalam laporan, saya tidak diarahkan ke detail bukti	543
Pembuatan laporan penilaian saya terjebak Sedang berlangsung status, dan saya tidak yakin bagaimana ini memengaruhi penagihan saya	544
Sumber daya tambahan	544
Kontrol pemecahan masalah dan set kontrol	544
Saya tidak dapat melihat kontrol atau kumpulan kontrol apa pun dalam penilaian saya	545
Saya tidak dapat mengunggah bukti manual ke kontrol	545
Apa artinya jika kontrol mengatakan “Penggantian tersedia”?	546
Saya perlu menggunakan beberapa AWS Config aturan sebagai sumber data untuk kontrol tunggal	546
Opsi aturan khusus tidak tersedia untuk sumber data saya	547
Daftar dropdown aturan khusus kosong	547
Saya tidak dapat melihat aturan khusus yang ingin saya gunakan	547
Saya tidak dapat melihat aturan terkelola yang ingin saya gunakan	549
Saya ingin berbagi kerangka kerja khusus, tetapi memiliki kontrol yang menggunakan AWS Config aturan khusus sebagai sumber data	551
Apa yang terjadi ketika aturan khusus diperbarui AWS Config?	552

Memecahkan masalah dasbor	554
Tidak ada data di dasbor saya	554
Opsi unduhan CSV tidak tersedia	555
Saya tidak melihat file yang diunduh saat mencoba mengunduh file CSV	555
Domain kontrol atau kontrol tertentu hilang dari dasbor	555
Saya melihat kontrol serupa atau duplikat muncul di bawah domain kontrol yang sama	555
Cuplikan harian menunjukkan jumlah bukti yang bervariasi setiap hari. Apakah ini normal? ..	557
Pemecahan masalah administrator yang didelegasikan dan AWS Organizations	557
Saya tidak dapat mengatur Audit Manager dengan akun administrator yang didelegasikan ..	558
Saat membuat penilaian, saya tidak dapat melihat akun dari organisasi saya di bawah Akun	
dalam cakupan	558
Saya mendapatkan akses ditolak kesalahan saat saya mencoba membuat laporan penilaian	
menggunakan akun administrator yang didelegasikan	559
Apa yang terjadi di Audit Manager jika saya memutuskan tautan akun anggota dari	
organisasi saya?	560
Apa yang terjadi jika saya menautkan ulang akun anggota ke organisasi saya?	560
Apa yang terjadi jika saya memigrasikan akun anggota dari satu organisasi ke organisasi	
lain?	560
Pencari bukti pemecahan masalah	561
Saya tidak dapat mengaktifkan pencari bukti	561
Saya mengaktifkan pencari bukti, tetapi saya tidak melihat bukti masa lalu di hasil pencarian	
saya	562
Saya tidak dapat menonaktifkan pencari bukti	562
Kueri pencarian saya gagal	563
Saya melihat bahwa domain kontrol ditandai sebagai “usang”. Apa artinya ini?	566
Saya tidak dapat membuat beberapa laporan penilaian dari hasil pencarian	566
Saya tidak dapat memasukkan bukti spesifik dari hasil pencarian saya	567
Tidak semua hasil pencari bukti saya disertakan dalam laporan penilaian	567
Saya ingin membuat laporan penilaian dari hasil pencarian saya, tetapi pernyataan kueri	
saya gagal	568
Sumber daya tambahan	571
Ekspor CSV saya gagal	571
Saya tidak dapat mengeksport bukti spesifik dari hasil pencarian saya	573
Saya tidak dapat mengeksport beberapa file CSV sekaligus	573
Kerangka pemecahan masalah	574

Pada halaman detail kerangka kerja kustom saya, saya diminta untuk membuat ulang kerangka kerja khusus saya	574
Saya tidak dapat membuat salinan kerangka kerja khusus saya	577
Status permintaan berbagi yang saya kirim ditampilkan sebagai Gagal	577
Permintaan berbagi saya memiliki titik biru di sebelahnya. Apa artinya ini?	578
Kerangka kerja bersama saya memiliki kontrol yang menggunakan kustom AWS Config aturan sebagai sumber data. Dapatkah penerima mengumpulkan bukti untuk kontrol ini?	580
Saya memperbarui aturan khusus yang digunakan dalam kerangka kerja bersama. Apakah saya perlu mengambil tindakan apa pun?	581
Memecahkan masalah notifikasi	582
Saya menentukan topik Amazon SNS di Audit Manager, tetapi saya tidak menerima pemberitahuan apa pun	583
Saya menentukan topik FIFO, tetapi saya tidak menerima notifikasi sesuai urutan yang diharapkan	583
Memecahkan masalah izin dan akses	583
Saya mengikuti prosedur penyiapan Audit Manager, tetapi saya tidak memiliki cukup hak IAM	584
Saya menentukan seseorang sebagai pemilik audit, tetapi mereka masih belum memiliki akses penuh ke penilaian. Mengapa ini?	585
Saya tidak dapat melakukan tindakan di Manajer Audit	585
Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses sumber daya Manajer Audit saya	585
Saya melihat kesalahan Akses Ditolak, meskipun memiliki izin Audit Manager yang diperlukan	586
Sumber daya tambahan	587
Memberi tag pada sumber daya	588
Sumber daya yang didukung	588
Batasan tag	589
Mengelola tag di Audit Manager	589
Kuota	591
Kuota Audit Manager default	591
Mengelola kuota Anda	592
Sumber daya tambahan	592
Contoh kode	594
Skenario	594
Buat kerangka kerja khusus dari paket AWS Config kesesuaian	595

Buat kerangka kerja khusus yang berisi kontrol CSPM Security Hub	599
Buat laporan penilaian	602
Keamanan	608
Perlindungan data	609
Penghapusan data Audit Manager	610
Enkripsi saat diam	611
Enkripsi saat bergerak	612
Manajemen kunci	612
Manajemen identitas dan akses	613
Audiens	614
Mengautentikasi dengan identitas	614
Mengelola akses menggunakan kebijakan	615
Bagaimana AWS Audit Manager bekerja dengan IAM	617
Identity-based contoh kebijakan	626
Cross-service pencegahan wakil yang bingung	642
Resource-based contoh kebijakan	644
AWS kebijakan yang dikelola	646
Pemecahan masalah	670
Menggunakan peran tertaut layanan	672
Validasi kepatuhan	686
Ketahanan	687
Keamanan infrastruktur	687
Titik akhir VPC (AWS PrivateLink)	688
Pertimbangan untuk AWS Audit Manager Titik akhir VPC	688
Membuat titik akhir antarmuka VPC untuk AWS Audit Manager	688
Membuat kebijakan titik akhir VPC untuk AWS Audit Manager	689
Pencatatan dan Pemantauan	690
Pemantauan EventBridge dengan Amazon	690
CloudTrail log	694
Konfigurasi dan kerentanan	697
Menonaktifkan AWS Audit Manager	698
Prosedur	698
Langkah berikutnya	700
Sumber daya tambahan	701
Riwayat dokumen	702

AWS Audit Manager Tidak lagi terbuka untuk pelanggan baru. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat perubahan [AWS Audit Manager ketersediaan](#).

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.

Apa itu AWS Audit Manager?

Selamat datang di Panduan AWS Audit Manager Pengguna.

AWS Audit Manager membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri. Audit Manager mengotomatiskan pengumpulan bukti sehingga Anda dapat lebih mudah menilai apakah kebijakan, prosedur, dan kegiatan Anda—juga dikenal sebagai kontrol — beroperasi secara efektif. Ketika tiba waktunya untuk audit, Manajer Audit membantu Anda mengelola tinjauan pemangku kepentingan atas kontrol Anda. Ini berarti Anda dapat membuat laporan siap audit dengan upaya manual yang jauh lebih sedikit.

Audit Manager menyediakan kerangka kerja bawaan yang menyusun dan mengotomatiskan penilaian untuk standar kepatuhan atau peraturan tertentu. Kerangka kerja mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan sesuai dengan persyaratan standar atau peraturan kepatuhan yang ditentukan. Anda juga dapat menyesuaikan kerangka kerja dan kontrol untuk mendukung audit internal sesuai dengan kebutuhan spesifik Anda.

Anda dapat membuat penilaian dari kerangka kerja apa pun. Saat Anda membuat penilaian, Audit Manager secara otomatis menjalankan penilaian sumber daya. Penilaian ini mengumpulkan data untuk Akun AWS yang Anda tentukan sebagai ruang lingkup audit Anda. Data yang dikumpulkan secara otomatis diubah menjadi bukti yang ramah audit. Kemudian, itu dilampirkan ke kontrol yang relevan untuk membantu Anda menunjukkan kepatuhan dalam keamanan, manajemen perubahan, kelangsungan bisnis, dan lisensi perangkat lunak. Proses pengumpulan bukti ini sedang berlangsung, dan dimulai saat Anda membuat penilaian Anda. Setelah Anda menyelesaikan audit dan Anda tidak lagi memerlukan Manajer Audit untuk mengumpulkan bukti, Anda dapat menghentikan pengumpulan bukti. Untuk melakukan ini, ubah status penilaian Anda menjadi tidak aktif.

Fitur Manajer Audit

Dengan AWS Audit Manager, Anda dapat melakukan tugas-tugas berikut:

- Memulai dengan cepat — [Buat penilaian pertama Anda](#) dengan memilih dari galeri kerangka kerja bawaan yang mendukung berbagai standar kepatuhan dan peraturan. Kemudian, mulai pengumpulan bukti otomatis untuk mengaudit Layanan AWS penggunaan Anda.

- Unggah dan kelola bukti dari lingkungan hibrida atau multicloud — Selain bukti yang dikumpulkan Audit Manager dari AWS lingkungan Anda, Anda juga dapat [mengunggah](#) dan mengelola bukti secara terpusat dari lingkungan lokal atau multicloud Anda.
- Mendukung standar dan peraturan kepatuhan umum - Pilih salah satu kerangka [AWS Audit Manager standar](#). Kerangka kerja ini menyediakan pemetaan kontrol bawaan untuk standar dan peraturan kepatuhan umum. Ini termasuk CIS Foundation Benchmark, PCI DSS, GDPR, HIPAA, SOC2, GxP, dan AWS praktik terbaik operasional.
- Pantau penilaian aktif Anda — Gunakan [dasbor Audit Manager](#) untuk melihat data analitik untuk penilaian aktif Anda, dan dengan cepat mengidentifikasi bukti yang tidak sesuai yang perlu diperbaiki.
- Cari bukti — Gunakan [Pencari bukti](#) fitur ini untuk menemukan bukti yang relevan dengan permintaan pencarian Anda dengan cepat. Anda dapat membuat laporan penilaian dari hasil penelusuran, atau mengekspor hasil pencarian Anda dalam format CSV.
- Buat kontrol khusus — [Buat kontrol Anda sendiri dari awal](#) atau [buat salinan kontrol standar atau kontrol](#) kustom yang dapat diedit. Anda juga dapat menggunakan fitur kontrol khusus untuk membuat pertanyaan penilaian risiko dan menyimpan tanggapan atas pertanyaan tersebut sebagai bukti manual.
- Petakan kontrol perusahaan Anda ke pengelompokan sumber AWS data yang telah ditentukan sebelumnya — Pilih kontrol umum yang mewakili tujuan Anda, dan gunakan kontrol tersebut untuk [membuat kontrol khusus](#) yang mengumpulkan bukti untuk portofolio kebutuhan kepatuhan Anda.
- Buat kerangka kerja khusus — [Buat kerangka kerja Anda sendiri](#) dengan kontrol standar atau kustom berdasarkan persyaratan spesifik Anda untuk audit internal.
- Bagikan kerangka kerja khusus — [Bagikan kerangka kerja Audit Manager kustom Anda](#) dengan Akun AWS yang lain, atau tiru ke Wilayah AWS yang lain di akun Anda sendiri.
- Mendukung kolaborasi lintas tim — [Delegasikan](#) kumpulan kontrol kepada pakar materi pelajaran yang dapat meninjau bukti terkait, menambahkan komentar, dan memperbarui status setiap kontrol.
- Buat laporan untuk auditor — [Hasilkan laporan penilaian](#) yang merangkum bukti relevan yang dikumpulkan untuk audit Anda dan tautkan ke folder yang berisi bukti terperinci.
- Memastikan integritas bukti — S <https://docs.aws.amazon.com/audit-manager/latest/userguide/settings-destination.html>impan bukti di lokasi yang aman, yang tetap tidak berubah.

 Note

AWS Audit Manager membantu mengumpulkan bukti yang relevan untuk memverifikasi kepatuhan terhadap standar dan peraturan kepatuhan tertentu. Namun, itu tidak menilai kepatuhan Anda sendiri. Bukti yang dikumpulkan oleh AWS Audit Manager karena itu mungkin tidak mencakup semua informasi tentang AWS penggunaan Anda yang diperlukan untuk audit. AWS Audit Manager bukan pengganti penasihat hukum atau pakar kepatuhan.

Harga untuk Manajer Audit

Untuk informasi lebih lanjut tentang harga, lihat [AWS Audit Manager Harga](#).

Apakah Anda pengguna Audit Manager pertama kali?

Jika Anda pertama kali menggunakan Audit Manager, kami sarankan Anda memulai dengan halaman berikut:

1. [Memahami AWS Audit Manager konsep dan terminologi](#) Pelajari tentang konsep dan istilah kunci yang digunakan dalam Audit Manager, seperti penilaian, kerangka kerja, dan kontrol.
2. [Memahami caranya AWS Audit Manager mengumpulkan bukti](#) Pelajari tentang bagaimana Manajer Audit mengumpulkan bukti untuk penilaian sumber daya.
3. [Pengaturan AWS Audit Manager dengan pengaturan yang disarankan](#) — Pelajari tentang persyaratan pengaturan untuk Manajer Audit.
4. [Memulai dengan AWS Audit Manager](#) — Ikuti tutorial untuk membuat penilaian Manajer Audit pertama Anda.
5. [AWS Audit Manager Referensi API](#) — Biasakan diri Anda dengan tindakan API Audit Manager dan tipe data.

Terkait Layanan AWS

AWS Audit Manager terintegrasi dengan beberapa Layanan AWS untuk secara otomatis mengumpulkan bukti yang dapat Anda sertakan dalam laporan penilaian Anda.

AWS Security Hub CSPM

AWS Security Hub CSPM memantau lingkungan Anda menggunakan pemeriksaan keamanan otomatis yang didasarkan pada praktik AWS terbaik dan standar industri. Audit Manager menangkap snapshot dari postur keamanan sumber daya Anda dengan melaporkan hasil pemeriksaan keamanan langsung dari Security Hub CSPM. Untuk informasi selengkapnya tentang Security Hub CSPM, lihat [Apa itu? AWS Security Hub CSPM](#) dalam Panduan AWS Security Hub CSPM Pengguna.

AWS CloudTrail

AWS CloudTrail membantu Anda memantau panggilan yang dilakukan ke AWS sumber daya di akun Anda. Ini termasuk panggilan yang dilakukan oleh AWS Management Console, AWS CLI, dan lainnya Layanan AWS. Audit Manager mengumpulkan data log secara CloudTrail langsung, dan mengubah log yang diproses menjadi bukti aktivitas pengguna. Untuk informasi selengkapnya CloudTrail, lihat [Apa itu AWS CloudTrail?](#) dalam Panduan AWS CloudTrail Pengguna.

AWS Config

AWS Config memberikan tampilan terperinci tentang konfigurasi sumber AWS daya di Akun AWS. Ini termasuk informasi tentang bagaimana sumber daya terkait satu sama lain dan bagaimana mereka dikonfigurasi di masa lalu. Audit Manager menangkap snapshot dari postur keamanan sumber daya Anda dengan melaporkan temuan langsung dari AWS Config. Untuk informasi selengkapnya AWS Config, lihat [Apa itu AWS Config?](#) dalam Panduan AWS Config Pengguna.

AWS License Manager

AWS License Manager merampingkan proses membawa lisensi vendor perangkat lunak ke cloud. Saat Anda membangun infrastruktur cloud AWS, Anda dapat menghemat biaya dengan menggunakan kembali inventaris lisensi yang ada untuk digunakan dengan sumber daya cloud. Audit Manager menyediakan kerangka kerja Manajer Lisensi untuk membantu Anda dengan persiapan audit Anda. Kerangka kerja ini terintegrasi dengan Manajer Lisensi untuk mengumpulkan informasi penggunaan lisensi berdasarkan aturan lisensi yang ditentukan pelanggan. Untuk informasi selengkapnya tentang Manajer Lisensi, lihat [Apa itu AWS License Manager?](#) dalam Panduan AWS License Manager Pengguna.

AWS Control Tower

AWS Control Tower memberlakukan pagar pembatas pencegahan dan detektif untuk infrastruktur cloud. Audit Manager menyediakan kerangka AWS Control Tower kerja Guardrails untuk membantu Anda dengan persiapan audit Anda. Kerangka kerja ini berisi semua AWS Config aturan yang

didasarkan pada pagar pembatas dari. AWS Control Tower Untuk informasi selengkapnya AWS Control Tower, lihat [Apa itu AWS Control Tower?](#) dalam Panduan AWS Control Tower Pengguna.

AWS Artifact

AWS Artifact adalah portal pengambilan artefak audit swalayan yang menyediakan akses sesuai permintaan ke dokumentasi kepatuhan dan sertifikasi untuk infrastruktur. AWS Artifact menawarkan bukti untuk membuktikan bahwa infrastruktur AWS Cloud memenuhi persyaratan kepatuhan. Sebaliknya, AWS Audit Manager membantu Anda mengumpulkan, meninjau, dan mengelola bukti untuk menunjukkan Layanan AWS bahwa penggunaan Anda sesuai. Untuk informasi selengkapnya AWS Artifact, lihat [Apa itu AWS Artifact?](#) dalam Panduan AWS Artifact Pengguna. Anda dapat mengunduh [daftar AWS laporan](#) di Konsol Manajemen AWS.

Amazon EventBridge

Amazon EventBridge membantu Anda mengotomatiskan Layanan AWS dan merespons secara otomatis peristiwa sistem seperti masalah ketersediaan aplikasi atau perubahan sumber daya. Anda dapat menggunakan EventBridge aturan untuk mendeteksi dan bereaksi terhadap peristiwa Audit Manager. Berdasarkan aturan yang Anda buat, memang EventBridge gil satu atau lebih tindakan target saat peristiwa cocok dengan nilai yang Anda tentukan dalam aturan. Untuk informasi selengkapnya, lihat [Memantau AWS Audit Manager dengan Amazon EventBridge](#).

Untuk daftar lingkup program kepatuhan tertentu, lihat [Layanan AWS di Lingkup berdasarkan Program Kepatuhan](#). Layanan AWS Untuk informasi lebih umum, lihat Program [AWS Kepatuhan](#).

Sumber daya Audit Manager lainnya

Jelajahi sumber daya berikut untuk mempelajari lebih lanjut tentang Manajer Audit.

- [Mengumpulkan Bukti dan Mengelola Data Audit Menggunakan AWS Audit Manager](#)
- [Integrasikan di seluruh Model Tiga Garis \(Bagian 2\): Ubah paket AWS Config kesesuaian menjadi AWS Audit Manager penilaian](#) dari Blog AWS Manajemen & Tata Kelola

Memahami AWS Audit Manager konsep dan terminologi

Untuk membantu Anda memulai, halaman ini mendefinisikan istilah dan menjelaskan beberapa konsep kunci AWS Audit Manager.

A

|B| | | |G|H| |J|K|L|M|N|O|P|Q| | |T|U|V|W|X|Y|Z

Penilaian

Anda dapat menggunakan penilaian Manajer Audit untuk secara otomatis mengumpulkan bukti yang relevan untuk audit.

Penilaian didasarkan pada kerangka kerja, yang merupakan pengelompokan kontrol yang terkait dengan audit Anda. Anda dapat membuat penilaian dari kerangka standar atau kerangka kerja khusus. Kerangka kerja standar berisi kumpulan kontrol bawaan yang mendukung standar kepatuhan atau peraturan tertentu. Sebaliknya, kerangka kerja khusus berisi kontrol yang dapat Anda sesuaikan dan dikelompokkan sesuai dengan persyaratan audit spesifik Anda. Menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian yang menentukan Akun AWS yang ingin Anda sertakan dalam ruang lingkup audit Anda.

Saat Anda membuat penilaian, Manajer Audit secara otomatis mulai menilai sumber daya di Akun AWS berdasarkan kontrol yang ditentukan dalam kerangka kerja. Selanjutnya, ia mengumpulkan bukti yang relevan dan mengubahnya menjadi format yang ramah auditor. Setelah melakukan ini, ia kemudian melampirkan bukti ke kontrol dalam penilaian Anda. Ketika tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan dan kemudian menambahkannya ke laporan penilaian. Laporan penilaian ini membantu Anda menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Pengumpulan bukti adalah proses berkelanjutan yang dimulai ketika Anda membuat penilaian Anda. Anda dapat menghentikan pengumpulan bukti dengan mengubah status penilaian menjadi tidak aktif. Atau, Anda dapat menghentikan pengumpulan bukti di tingkat kontrol. Anda dapat melakukan ini dengan mengubah status kontrol tertentu dalam penilaian Anda menjadi tidak aktif.

Untuk petunjuk tentang cara membuat dan mengelola penilaian, lihat [Mengelola penilaian di AWS Audit Manager](#).

Laporan penilaian

Laporan penilaian adalah dokumen akhir yang dihasilkan dari penilaian Manajer Audit. Laporan ini merangkum bukti relevan yang dikumpulkan untuk audit Anda. Mereka menautkan ke folder bukti yang relevan. Folder diberi nama dan diatur sesuai dengan kontrol yang ditentukan dalam penilaian Anda. Untuk setiap penilaian, Anda dapat meninjau bukti yang dikumpulkan oleh Manajer Audit, dan memutuskan bukti mana yang ingin Anda sertakan dalam laporan penilaian.

Untuk mempelajari lebih lanjut tentang laporan penilaian, lihat [Laporan penilaian](#). Untuk mempelajari cara membuat laporan penilaian, lihat [Menyiapkan laporan penilaian di AWS Audit Manager](#).

Tujuan laporan penilaian

Tujuan laporan penilaian adalah bucket S3 default tempat Audit Manager menyimpan laporan penilaian Anda. Untuk mempelajari selengkapnya, lihat [Mengkonfigurasi tujuan laporan penilaian default](#).

Audit

Audit adalah pemeriksaan independen terhadap aset, operasi, atau integritas bisnis organisasi Anda. Audit teknologi informasi (TI) secara khusus memeriksa kontrol dalam sistem informasi organisasi Anda. Tujuan dari audit TI adalah untuk menentukan apakah sistem informasi melindungi aset, beroperasi secara efektif, dan menjaga integritas data. Semua ini penting untuk memenuhi persyaratan peraturan yang diamanatkan oleh standar kepatuhan atau peraturan.

Pemilik audit

Istilah pemilik audit memiliki dua arti yang berbeda tergantung pada konteksnya.

Dalam konteks Manajer Audit, pemilik audit adalah pengguna atau peran yang mengelola penilaian dan sumber daya terkait. Tanggung jawab persona Manajer Audit ini termasuk membuat penilaian, meninjau bukti, dan menghasilkan laporan penilaian. Audit Manager adalah layanan kolaboratif, dan pemilik audit mendapat manfaat ketika pemangku kepentingan lain berpartisipasi dalam penilaian mereka. Misalnya, Anda dapat menambahkan pemilik audit lain ke penilaian Anda untuk berbagi tugas manajemen. Atau, jika Anda adalah pemilik audit dan Anda memerlukan bantuan untuk menafsirkan bukti yang dikumpulkan untuk suatu kontrol, Anda dapat [mendelegasikan kumpulan kontrol tersebut](#) kepada pemangku kepentingan yang memiliki keahlian materi pelajaran di bidang tersebut. Orang seperti itu dikenal sebagai persona delegasi.

Dalam istilah bisnis, pemilik audit adalah seseorang yang mengoordinasikan dan mengawasi upaya kesiapan audit perusahaan mereka, dan menyajikan bukti kepada auditor. Biasanya, ini adalah profesional tata kelola, risiko, dan kepatuhan (GRC), seperti Petugas Kepatuhan atau Petugas Perlindungan Data GDPR. Profesional GRC memiliki keahlian dan wewenang untuk mengelola persiapan audit. Lebih khusus lagi, mereka memahami persyaratan kepatuhan, dan dapat menganalisis, menafsirkan, dan menyiapkan data pelaporan. Namun, peran bisnis lain juga dapat mengambil persona Manajer Audit dari pemilik audit—tidak hanya profesional GRC yang mengambil peran ini. Misalnya, Anda dapat memilih agar penilaian Manajer Audit diatur dan dikelola oleh pakar teknis dari salah satu tim berikut:

- SecOps
- IT/DevOps
- Respon Operasi Center/Incident Keamanan
- Tim serupa yang memiliki, mengembangkan, memperbaiki, dan menerapkan aset cloud, dan memahami infrastruktur cloud organisasi Anda

Siapa yang Anda pilih untuk ditugaskan sebagai pemilik audit dalam penilaian Manajer Audit Anda sangat bergantung pada organisasi Anda. Itu juga tergantung pada bagaimana Anda menyusun operasi keamanan Anda dan spesifikasi audit. Dalam Audit Manager, individu yang sama dapat mengasumsikan persona pemilik audit dalam satu penilaian, dan persona delegasi dalam penilaian lain.

Tidak peduli bagaimana Anda memilih untuk menggunakan Audit Manager, Anda dapat mengelola pemisahan tugas di seluruh organisasi menggunakan owner/delegate persona audit dan memberikan kebijakan IAM tertentu kepada setiap pengguna. Melalui pendekatan dua langkah ini, Manajer Audit memastikan bahwa Anda memiliki kontrol penuh atas semua spesifikasi penilaian individu. Untuk informasi selengkapnya, lihat [Kebijakan yang disarankan untuk persona pengguna di AWS Audit Manager](#).

AWS sumber yang dikelola

Sumber AWS terkelola adalah sumber bukti yang AWS disimpan untuk Anda.

Setiap sumber AWS terkelola adalah pengelompokan sumber data yang telah ditentukan sebelumnya yang dipetakan ke kontrol umum atau kontrol inti tertentu. Ketika Anda menggunakan kontrol umum sebagai sumber bukti, Anda secara otomatis mengumpulkan bukti untuk semua kontrol inti yang mendukung kontrol umum itu. Anda juga dapat menggunakan kontrol inti individu sebagai sumber bukti.

Setiap kali sumber AWS terkelola diperbarui, pembaruan yang sama secara otomatis diterapkan ke semua kontrol kustom yang menggunakan sumber terkel AWS tersebut. Ini berarti bahwa kontrol khusus Anda mengumpulkan bukti terhadap definisi terbaru dari sumber bukti tersebut. Ini membantu Anda memastikan kepatuhan berkelanjutan saat lingkungan kepatuhan cloud berubah.

Lihat juga: [customer managed source](#), [evidence source](#).

C

|B| | | |G|H| |J|K|L|M|N|O|P|Q| | |T|U|V|W|X|Y|Z

Log perubahan

Untuk setiap kontrol dalam penilaian, Audit Manager melacak aktivitas pengguna untuk kontrol tersebut. Anda kemudian dapat meninjau jejak audit aktivitas yang terkait dengan kontrol tertentu. Untuk informasi selengkapnya tentang aktivitas pengguna yang ditangkap di changelog, lihat. [Tab Changelog](#)

Kepatuhan cloud

Kepatuhan cloud adalah prinsip umum bahwa sistem yang dikirimkan cloud harus sesuai dengan standar yang dihadapi oleh pelanggan cloud.

Kontrol umum

Lihat [control](#).

Peraturan kepatuhan

Peraturan kepatuhan adalah hukum, aturan, atau perintah lain yang ditentukan oleh otoritas, biasanya untuk mengatur perilaku. Salah satu contohnya adalah GDPR.

Standar kepatuhan

Standar kepatuhan adalah seperangkat pedoman terstruktur yang merinci proses organisasi untuk mempertahankan sesuai dengan peraturan, spesifikasi, atau undang-undang yang ditetapkan. Contohnya termasuk PCI DSS dan HIPAA.

Kontrol

Kontrol adalah pengamanan atau penanggulangan yang ditentukan untuk sistem informasi atau organisasi. Kontrol dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi Anda, dan untuk memenuhi serangkaian persyaratan yang ditentukan. Mereka memberikan jaminan bahwa sumber daya Anda beroperasi sebagaimana dimaksud, data Anda dapat diandalkan, dan organisasi Anda mematuhi hukum dan peraturan yang berlaku.

Dalam Audit Manager, kontrol juga dapat mewakili pertanyaan dalam kuesioner penilaian risiko vendor. Dalam hal ini, kontrol adalah pertanyaan spesifik yang menanyakan informasi tentang postur keamanan dan kepatuhan organisasi.

Kontrol mengumpulkan bukti secara terus-menerus saat mereka aktif dalam penilaian Manajer Audit Anda. Anda juga dapat menambahkan bukti secara manual ke kontrol apa pun. Setiap bukti adalah catatan yang membantu Anda menunjukkan kepatuhan terhadap persyaratan kontrol.

Audit Manager menyediakan jenis kontrol berikut:

Jenis kontrol	Deskripsi
Kontrol umum	Anda dapat menganggap kontrol umum sebagai tindakan yang membantu Anda memenuhi tujuan kontrol. Karena kontrol umum tidak khusus untuk standar kepatuhan apa pun, kontrol ini membantu Anda mengumpulkan bukti yang dapat mendukung berbagai kewajiban kepatuhan yang tumpang tindih. Misalnya, katakanlah Anda memiliki tujuan kontrol yang disebut Klasifikasi dan penanganan data. Untuk memenuhi tujuan ini, Anda dapat menerapkan kontrol umum yang disebut kontrol akses untuk memantau dan mendeteksi akses tidak sah ke sumber daya Anda. • Kontrol umum otomatis mengumpulkan bukti untuk Anda. Mereka terdiri dari pengelompokan satu atau lebih kontrol inti terkait. Pada gilirannya, masing-masing kontrol inti ini secara otomatis mengumpulkan bukti yang relevan dari kelompok sumber AWS data yang telah ditentukan sebelumnya. AWS mengelola sumber data yang mendasari ini untuk Anda, dan memperbaruinya setiap kali peraturan dan standar berubah dan sumber data baru diidentifikasi. • Kontrol umum manual mengharuskan Anda mengunggah bukti Anda sendiri. Ini karena mereka biasanya memerlukan penyediaan catatan fisik, atau detail tentang peristiwa yang terjadi di luar AWS lingkungan Anda. Untuk alasan ini, seringkali tidak ada sumber AWS data yang dapat menghasilkan bukti untuk mendukung persyaratan kontrol umum manual. Anda tidak dapat mengedit kontrol umum. Namun, Anda dapat menggunakan kontrol umum apa pun sebagai sumber bukti saat membuat kontrol kustom.
Kontrol inti	Ini adalah pedoman preskriptif untuk AWS lingkungan Anda. Anda dapat menganggap kontrol inti sebagai tindakan yang membantu Anda memenuhi persyaratan kontrol umum. Misalnya, katakanlah Anda menggunakan kontrol umum yang disebut Kontrol akses untuk memantau akses tidak sah ke sumber daya Anda. Untuk mendukung kontrol umum ini, Anda dapat menggunakan kontrol inti yang disebut Blokir akses baca publik di bucket S3.

Jenis kontrol	Deskripsi
	Karena kontrol inti tidak spesifik untuk standar kepatuhan apa pun, mereka mengumpulkan bukti yang dapat mendukung berbagai kewajiban kepatuhan yang tumpang tindih. Setiap kontrol inti menggunakan satu atau lebih sumber data untuk mengumpulkan bukti tentang yang spesifik Layanan AWS. AWS mengelola sumber data yang mendasari ini untuk Anda, dan memperbaruinya setiap kali peraturan dan standar berubah dan sumber data baru diidentifikasi. Anda tidak dapat mengedit kontrol inti. Namun, Anda dapat menggunakan kontrol inti apa pun sebagai sumber bukti saat membuat kontrol kustom.
Kontrol standar	Ini adalah kontrol bawaan yang disediakan oleh Audit Manager. Anda dapat menggunakan kontrol standar untuk membantu persiapan audit untuk standar kepatuhan tertentu. Setiap kontrol standar terkait dengan standar tertentu framework di Audit Manager, dan mengumpulkan bukti yang dapat Anda gunakan untuk menunjukkan kepatuhan terhadap kerangka kerja tersebut. Kontrol standar mengumpulkan bukti dari sumber data yang mendasari yang AWS mengelola. Sumber data ini secara otomatis diperbarui setiap kali peraturan dan standar berubah dan sumber data baru diidentifikasi. Anda tidak dapat mengedit kontrol standar. Namun, Anda dapat membuat salinan kontrol standar yang dapat diedit.
Kontrol kustom	Ini adalah kontrol yang Anda buat di Audit Manager untuk memenuhi persyaratan kepatuhan spesifik Anda. Anda dapat membuat kontrol kustom dari awal, atau membuat salinan kontrol standar yang ada yang dapat diedit. Saat Anda membuat kontrol khusus, Anda dapat menentukan evidence source s tertentu yang menentukan dari mana Audit Manager mengumpulkan bukti. Setelah Anda membuat kontrol kustom, Anda dapat mengedit kontrol itu atau menambahkannya ke kerangka kerja khusus. Anda juga dapat membuat salinan kontrol kustom yang dapat diedit.

Domain kontrol

Anda dapat menganggap domain kontrol sebagai kategori kontrol yang tidak spesifik untuk standar kepatuhan apa pun. Contoh domain kontrol adalah perlindungan data.

Kontrol sering dikelompokkan berdasarkan domain untuk tujuan organisasi yang sederhana. Setiap domain memiliki beberapa tujuan.

Pengelompokan domain kontrol adalah salah satu fitur paling kuat dari dasbor <https://docs.aws.amazon.com/audit-manager/latest/userguide/dashboard.html> Audit Manager. Audit Manager menyoroti kontrol dalam penilaian Anda yang memiliki bukti yang tidak sesuai, dan mengelompokkannya berdasarkan domain kontrol. Ini memungkinkan Anda untuk memfokuskan upaya remediasi Anda pada domain subjek tertentu saat Anda mempersiapkan audit.

Tujuan kontrol

Tujuan kontrol menggambarkan tujuan dari kontrol umum yang berada di bawahnya. Setiap tujuan dapat memiliki beberapa kontrol umum. Jika kontrol umum ini berhasil diterapkan, mereka akan membantu Anda memenuhi tujuan.

Setiap tujuan kontrol berada di bawah domain kontrol. Misalnya, domain kontrol perlindungan data mungkin memiliki tujuan kontrol bernama Klasifikasi dan penanganan Data. Untuk mendukung tujuan kontrol ini, Anda dapat menggunakan kontrol umum yang disebut kontrol akses untuk memantau dan mendeteksi akses tidak sah ke sumber daya Anda.

Kontrol inti

Lihat [control](#).

Kontrol kustom

Lihat [control](#).

Sumber yang dikelola pelanggan

Sumber yang dikelola pelanggan adalah sumber bukti yang Anda tentukan.

Saat Anda membuat kontrol kustom di Audit Manager, Anda dapat menggunakan opsi ini untuk membuat sumber data individual Anda sendiri. Ini memberi Anda fleksibilitas untuk mengumpulkan bukti otomatis dari sumber daya khusus bisnis, seperti AWS Config aturan khusus. Anda juga dapat menggunakan opsi ini jika ingin menambahkan bukti manual ke kontrol kustom Anda.

Saat Anda menggunakan sumber yang dikelola pelanggan, Anda bertanggung jawab untuk memelihara semua sumber data yang Anda buat.

Lihat juga: [AWS managed source](#), [evidence source](#).

D

|B| | | |G|H| |J|K|L|M|N|O|P|Q| | |T|U|V|W|X|Y|Z

Sumber data

Audit Manager menggunakan sumber data untuk mengumpulkan bukti untuk kontrol. Sumber data memiliki properti berikut:

- Jenis sumber data mendefinisikan jenis sumber data dari mana Audit Manager mengumpulkan bukti.
 - Untuk bukti otomatis, jenisnya bisa berupa AWS Security Hub CSPM, AWS Config, AWS CloudTrail, atau panggilan AWS API.
 - Jika Anda mengunggah bukti Anda sendiri, jenisnya adalah Manual.
 - Audit Manager API mengacu pada tipe sumber data sebagai [Source](#) Type.
- Pemetaan sumber data adalah kata kunci yang menunjukkan dari mana bukti dikumpulkan untuk jenis sumber data tertentu.
 - Misalnya, ini mungkin nama CloudTrail acara atau nama AWS Config aturan.
 - Audit Manager API mengacu pada pemetaan sumber data sebagai [SourceKeyword](#).
- Nama sumber data memberi label pada pasangan jenis sumber data dan pemetaan.
 - Untuk kontrol standar, Audit Manager menyediakan nama default.
 - Untuk kontrol khusus, Anda dapat memberikan nama Anda sendiri.
 - Audit Manager API mengacu pada nama sumber data sebagai [SourceName](#).

Kontrol tunggal dapat memiliki beberapa jenis sumber data dan beberapa pemetaan. Misalnya, satu kontrol mungkin mengumpulkan bukti dari campuran jenis sumber data (seperti AWS Config dan Security Hub CSPM). Kontrol lain AWS Config mungkin memiliki satu-satunya jenis sumber data, dengan beberapa AWS Config aturan sebagai pemetaan.

Tabel berikut mencantumkan jenis sumber data otomatis dan menunjukkan contoh beberapa pemetaan yang sesuai.

Jenis sumber data	Deskripsi	Contoh pemetaan
AWS Security Hub CSPM	Gunakan jenis sumber data ini untuk mengambil snapshot dari postur	EC2.1

Jenis sumber data	Deskripsi	Contoh pemetaan
	keamanan sumber daya Anda. Audit Manager menggunakan nama kontrol CSPM Security Hub sebagai kata kunci pemetaan, dan melaporkan hasil pemeriksaan keamanan tersebut langsung dari Security Hub CSPM.	
AWS Config	Gunakan jenis sumber data ini untuk mengambil snapshot dari postur keamanan sumber daya Anda. Audit Manager menggunakan nama AWS Config aturan sebagai kata kunci pemetaan, dan melaporkan hasil pemeriksaan aturan tersebut langsung dari AWS Config.	SNS_ENCRYPTED_KMS

Jenis sumber data	Deskripsi	Contoh pemetaan
AWS CloudTrail	Gunakan jenis sumber data ini untuk melacak aktivitas pengguna tertentu yang diperlukan dalam audit Anda. Audit Manager menggunakan nama CloudTrail acara sebagai kata kunci pemetaan, dan mengumpulkan aktivitas pengguna terkait dari CloudTrail log Anda.	CreateAccessKey
AWS Panggilan API	Gunakan jenis sumber data ini untuk mengambil snapshot konfigurasi sumber daya Anda melalui panggilan API ke suatu sumber tertentu Layanan AWS. Audit Manager menggunakan nama panggilan API sebagai kata kunci pemetaan, dan mengumpulkan respons API.	kms_ListKeys

Delegasi

Delegasi adalah AWS Audit Manager pengguna dengan izin terbatas. Delegasi biasanya memiliki keahlian bisnis atau teknis khusus. Misalnya, keahlian ini mungkin dalam kebijakan retensi data, rencana pelatihan, infrastruktur jaringan, atau manajemen identitas. Delegasi membantu pemilik audit meninjau bukti yang dikumpulkan untuk kontrol yang ada di bidang keahlian mereka. Delegasi dapat meninjau kumpulan kontrol dan bukti terkaitnya, menambahkan komentar, mengunggah bukti tambahan, dan memperbarui status masing-masing kontrol yang Anda tetapkan kepada mereka untuk ditinjau.

Pemilik audit menetapkan kumpulan kontrol tertentu untuk delegasi, bukan seluruh penilaian. Akibatnya, delegasi memiliki akses terbatas ke penilaian. Untuk petunjuk tentang cara mendelegasikan kumpulan kontrol, lihat [Delegasi di AWS Audit Manager](#).

E

| B | | | | G | H | | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Bukti

Bukti adalah catatan yang berisi informasi yang diperlukan untuk menunjukkan kepatuhan terhadap persyaratan kontrol. Contoh bukti termasuk aktivitas perubahan yang dipanggil oleh pengguna, dan snapshot konfigurasi sistem.

Ada dua jenis bukti utama dalam Audit Manager: bukti otomatis dan bukti manual.

Jenis bukti	Deskripsi
Bukti otomatis	Ini adalah bukti yang dikumpulkan oleh Manajer Audit secara otomatis. Ini termasuk tiga kategori bukti otomatis berikut: 1. Pemeriksaan kepatuhan — Hasil pemeriksaan kepatuhan diambil dari AWS Security Hub CSPM, AWS Config, atau keduanya. Contoh pemeriksaan kepatuhan termasuk hasil pemeriksaan keamanan dari Security Hub CSPM untuk kontrol PCI DSS, dan evaluasi AWS Config aturan untuk kontrol HIPAA. Untuk informasi selengkapnya, lihat Aturan AWS Config didukung oleh AWS Audit Manager dan AWS Security Hub CSPM kontrol didukung oleh AWS Audit Manager. 2. Aktivitas pengguna — Aktivitas pengguna yang mengubah konfigurasi sumber daya diambil dari CloudTrail log saat aktivitas itu terjadi. Contoh aktivitas pengguna termasuk pembaruan tabel rute, perubahan pengaturan cadangan instans Amazon RDS, dan perubahan kebijakan enkripsi bucket S3. Untuk informasi selengkapnya, lihat AWS CloudTrail nama acara didukung oleh AWS Audit Manager.

Jenis bukti	Deskripsi
	3. Data konfigurasi — Sebuah snapshot dari konfigurasi sumber daya diambil langsung dari setiap hari, mingguan, atau bulanan. Layanan AWS Contoh snapshot konfigurasi termasuk daftar rute untuk tabel rute VPC, pengaturan cadangan instans Amazon RDS, dan kebijakan enkripsi bucket S3. Untuk informasi selengkapnya, lihat AWS Panggilan API didukung oleh AWS Audit Manager.
Bukti manual	Ini adalah bukti yang Anda tambahkan ke Manajer Audit sendiri. Ada tiga cara untuk menambahkan bukti Anda sendiri: 1. Impor file dari Amazon S3 2. Unggah file dari browser Anda 3. Masukkan tanggapan teks untuk pertanyaan penilaian risiko Untuk informasi selengkapnya, lihat Menambahkan bukti manual di AWS Audit Manager.

Pengumpulan bukti otomatis dimulai saat Anda membuat penilaian. Ini adalah proses yang berkelanjutan, dan Manajer Audit mengumpulkan bukti pada frekuensi yang berbeda tergantung pada jenis bukti dan sumber data yang mendasarinya. Untuk informasi selengkapnya, lihat [Memahami caranya AWS Audit Manager mengumpulkan bukti](#).

Untuk petunjuk tentang cara meninjau bukti dalam penilaian, lihat [Meninjau bukti di AWS Audit Manager](#).

Sumber bukti

Sumber bukti mendefinisikan dari mana kontrol mengumpulkan bukti. Ini dapat berupa sumber data individu, atau pengelompokan sumber data yang telah ditentukan yang dipetakan ke kontrol umum atau kontrol inti.

Saat membuat kontrol kustom, Anda dapat mengumpulkan bukti dari sumber terkel AWS ola, sumber yang dikelola pelanggan, atau keduanya.

 Tip

Kami menyarankan Anda menggunakan sumber ter AWS kelola. Setiap kali AWS sumber terkelola diperbarui, pembaruan yang sama secara otomatis diterapkan ke semua kontrol kustom yang menggunakan sumber ini. Ini berarti bahwa kontrol khusus Anda selalu mengumpulkan bukti terhadap definisi terbaru dari sumber bukti tersebut. Ini membantu Anda memastikan kepatuhan berkelanjutan saat lingkungan kepatuhan cloud berubah.

Lihat juga: [AWS managed source](#), [customer managed source](#).

Metode pengumpulan bukti

Ada dua cara kontrol dapat mengumpulkan bukti.

Metode pengumpulan bukti	Deskripsi
Otomatis	Kontrol otomatis secara otomatis mengumpulkan bukti dari sumber AWS data. Bukti otomatis ini dapat membantu Anda menunjukkan kepatuhan penuh atau sebagian dengan kontrol.
Manual	Kontrol manual mengharuskan Anda mengunggah bukti Anda sendiri untuk menunjukkan kepatuhan terhadap kontrol.

 Note

Anda dapat melampirkan bukti manual ke kontrol otomatis apa pun. Dalam banyak kasus, kombinasi bukti otomatis dan manual diperlukan untuk menunjukkan kepatuhan penuh terhadap kontrol. Meskipun Manajer Audit dapat memberikan bukti otomatis yang bermanfaat dan relevan, beberapa bukti otomatis mungkin hanya menunjukkan kepatuhan sebagian. Dalam hal ini, Anda dapat melengkapi bukti otomatis yang disediakan Manajer Audit dengan bukti Anda sendiri.

Contoh:

- Ini [AWS Kerangka Praktik Terbaik AI Generatif v2](#) berisi kontrol yang disebut `Error analysis`. Kontrol ini mengharuskan Anda mengidentifikasi kapan ketidakakuratan

terdeteksi dalam penggunaan model Anda. Ini juga mengharuskan Anda untuk melakukan analisis kesalahan menyeluruh untuk memahami akar penyebab dan mengambil tindakan korektif.

- Untuk mendukung kontrol ini, Audit Manager mengumpulkan bukti otomatis yang menunjukkan apakah CloudWatch alarm diaktifkan untuk Akun AWS tempat penilaian Anda berjalan. Anda dapat menggunakan bukti ini untuk menunjukkan kepatuhan sebagian dengan kontrol dengan membuktikan bahwa alarm dan cek Anda dikonfigurasi dengan benar.
- Untuk menunjukkan kepatuhan penuh, Anda dapat melengkapi bukti otomatis dengan bukti manual. Misalnya, Anda dapat mengunggah kebijakan atau prosedur yang menunjukkan proses analisis kesalahan, ambang batas untuk eskalasi dan pelaporan, dan hasil analisis akar penyebab Anda. Anda dapat menggunakan bukti manual ini untuk menunjukkan bahwa kebijakan yang ditetapkan sudah ada, dan tindakan korektif telah diambil saat diminta.

Untuk contoh yang lebih rinci, lihat [Kontrol dengan sumber data campuran](#).

Tujuan ekspor

Tujuan ekspor adalah bucket S3 default tempat Audit Manager menyimpan file yang Anda ekspor dari pencari bukti. Untuk informasi selengkapnya, lihat [Mengkonfigurasi tujuan ekspor default Anda untuk pencari bukti](#).

F

|B| | | |G|H| |J|K|L|M|N|O|P|Q| | |T|U|V|W|X|Y|Z

Kerangka

Kerangka kerja Manajer Audit menyusun dan mengotomatiskan penilaian untuk standar atau prinsip tata kelola risiko tertentu. Kerangka kerja ini mencakup kumpulan kontrol bawaan atau yang ditentukan pelanggan, dan mereka membantu Anda memetakan AWS sumber daya Anda dengan persyaratan kontrol ini.

Ada dua jenis kerangka kerja dalam Audit Manager.

Jenis kerangka kerja	Deskripsi
Kerangka standar	Ini adalah kerangka kerja bawaan yang didasarkan pada praktik AWS terbaik untuk berbagai standar kepatuhan dan peraturan. Anda dapat menggunakan kerangka kerja standar untuk membantu persiapan audit untuk standar atau peraturan kepatuhan tertentu, seperti PCI DSS atau HIPAA.
Kerangka kerja khusus	Ini adalah kerangka kerja khusus yang Anda definisikan sebagai pengguna Audit Manager. Anda dapat menggunakan kerangka kerja khusus untuk membantu persiapan audit sesuai dengan persyaratan GRC spesifik Anda.

Untuk petunjuk tentang cara membuat dan mengelola kerangka kerja, lihat [Menggunakan pustaka kerangka kerja untuk mengelola kerangka kerja di AWS Audit Manager](#).

Note

AWS Audit Manager membantu mengumpulkan bukti yang relevan untuk memverifikasi kepatuhan terhadap standar dan peraturan kepatuhan tertentu. Namun, itu tidak menilai kepatuhan Anda sendiri. Bukti yang dikumpulkan oleh AWS Audit Manager karena itu mungkin tidak mencakup semua informasi tentang AWS penggunaan Anda yang diperlukan untuk audit. AWS Audit Manager bukan pengganti penasihat hukum atau pakar kepatuhan.

Berbagi kerangka kerja

Anda dapat menggunakan [Berbagi kerangka kerja khusus di AWS Audit Manager](#) fitur ini untuk dengan cepat membagikan kerangka kerja kustom Anda di seluruh Akun AWS dan Wilayah. Untuk berbagi kerangka kerja khusus, Anda membuat permintaan berbagi. Penerima kemudian memiliki 120 hari untuk menerima atau menolak permintaan. Ketika mereka menerima, Audit Manager mereplikasi kerangka kerja khusus bersama ke perpustakaan kerangka kerja mereka. Selain mereplikasi kerangka kerja khusus, Audit Manager juga mereplikasi kumpulan kontrol kustom dan kontrol yang terkandung dalam kerangka kerja tersebut. Kontrol kustom ini

ditambahkan ke pustaka kontrol penerima. Audit Manager tidak mereplikasi kerangka kerja atau kontrol standar. Ini karena sumber daya ini sudah tersedia secara default di setiap akun dan Wilayah.

I

| B | | | | G | H | | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Bukti tidak meyakinkan

AWS Audit Manager Menandai bukti sebagai tidak meyakinkan ketika evaluasi kepatuhan otomatis tidak memungkinkan. Ini terjadi dalam situasi berikut:

- Anda belum mengaktifkan AWS Config atau AWS Security Hub CSPM, yang merupakan sumber data utama.
- Bukti dikumpulkan langsung dari AWS layanan melalui panggilan API, AWS CloudTrail log, atau unggahan manual.

Ketika tidak ada mekanisme untuk evaluasi otomatis bukti ini, tidak AWS Audit Manager dapat memberikan rincian evaluasi. Akibatnya, itu menandai bukti sebagai tidak meyakinkan.

Important

Bukti yang tidak meyakinkan tidak menunjukkan kegagalan. Sebaliknya, ini menandakan bahwa Anda perlu mengevaluasi bukti kepatuhan secara manual.

R

| B | | | | G | H | | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Sumber daya

Sumber daya adalah aset fisik atau informasi yang dinilai dalam audit. Contoh sumber AWS daya termasuk instans Amazon EC2, instans Amazon RDS, bucket Amazon S3, dan subnet Amazon VPC.

Penilaian sumber daya

Penilaian sumber daya adalah proses menilai sumber daya individu. Penilaian ini didasarkan pada persyaratan kontrol. Sementara penilaian aktif, Manajer Audit menjalankan penilaian

sumber daya untuk setiap sumber daya individu dalam lingkup penilaian. Penilaian sumber daya menjalankan serangkaian tugas berikut:

1. Mengumpulkan bukti termasuk konfigurasi sumber daya, log peristiwa, dan temuan
2. Menerjemahkan dan memetakan bukti ke kontrol
3. Menyimpan dan melacak garis keturunan bukti untuk memungkinkan integritas

Kepatuhan sumber daya

Kepatuhan sumber daya mengacu pada status evaluasi sumber daya yang dinilai saat mengumpulkan bukti pemeriksaan kepatuhan.

Audit Manager mengumpulkan bukti pemeriksaan kepatuhan untuk kontrol yang menggunakan AWS Config dan Security Hub CSPM sebagai jenis sumber data. Beberapa sumber daya dapat dinilai selama pengumpulan bukti ini. Akibatnya, satu bukti pemeriksaan kepatuhan dapat mencakup satu atau lebih sumber daya.

Anda dapat menggunakan filter kepatuhan sumber daya di pencari bukti untuk menjelajahi status kepatuhan di tingkat sumber daya. Setelah pencarian selesai, Anda dapat melihat pratinjau sumber daya yang cocok dengan permintaan pencarian Anda.

Dalam pencari bukti, ada tiga nilai yang mungkin untuk kepatuhan sumber daya:

Nilai	Deskripsi
Non-compliant	Ini mengacu pada sumber daya dengan masalah pemeriksaan kepatuhan. Ini terjadi jika Hub Keamanan melaporkan hasil Gagal untuk sumber daya, atau jika AWS Config melaporkan Non-compliant hasilnya.
Sesuai	Ini mengacu pada sumber daya yang tidak memiliki masalah pemeriksaan kepatuhan. Ini terjadi jika Security Hub CSPM melaporkan hasil Pass untuk sumber daya, atau jika AWS Config melaporkan hasil Compliant.
Tidak meyakinkan	Ini mengacu pada sumber daya yang pemeriksaan kepatuhannya tidak tersedia atau tidak berlaku. Ini terjadi jika AWS Config atau Security Hub CSPM adalah tipe sumber data yang mendasarinya, tetapi layanan tersebut tidak diaktifkan.

Nilai	Deskripsi
	Ini juga terjadi jika jenis sumber data yang mendasarinya tidak mendukung pemeriksaan kepatuhan (seperti bukti manual, panggilan AWS API, atau CloudTrail).

D

| B | | | | G | H | | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Layanan dalam lingkup

Manajer Audit mengelola yang Layanan AWS berada dalam ruang lingkup penilaian Anda. Jika Anda memiliki penilaian yang lebih lama, mungkin saja Anda secara manual menentukan layanan dalam cakupan di masa lalu. Setelah 04 Juni 2024, Anda tidak dapat secara manual menentukan atau mengedit layanan dalam cakupan.

Layanan dalam ruang lingkup Layanan AWS adalah tempat penilaian Anda mengumpulkan buktinya. Ketika layanan disertakan dalam lingkup penilaian Anda, Manajer Audit menilai sumber daya layanan tersebut. Beberapa contoh sumber daya termasuk yang berikut:

- Instans Amazon EC2
- Sebuah ember S3
- Pengguna atau peran IAM
- Tabel DynamoDB
- Komponen jaringan seperti Amazon Virtual Private Cloud (VPC), grup keamanan, atau tabel daftar kontrol akses jaringan (ACL)

Misalnya, jika Amazon S3 adalah layanan dalam cakupan, Audit Manager dapat mengumpulkan bukti tentang bucket S3 Anda. Bukti pasti yang dikumpulkan ditentukan oleh kontrol [data source](#). Misalnya, jika tipe sumber data adalah AWS Config, dan pemetaan sumber data adalah AWS Config aturan (seperti `s3-bucket-public-write-prohibited`), Audit Manager mengumpulkan hasil evaluasi aturan tersebut sebagai bukti.

Note

Perlu diingat bahwa layanan dalam lingkup berbeda dengan jenis sumber data, yang juga bisa berupa Layanan AWS atau sesuatu yang lain. Untuk informasi selengkapnya, lihat

[Apa perbedaan antara layanan dalam ruang lingkup dan tipe sumber data?](#) di bagian Pemecahan Masalah pada panduan ini.

Kontrol standar

Lihat [control](#).

Memahami caranya AWS Audit Manager mengumpulkan bukti

Setiap penilaian aktif secara AWS Audit Manager otomatis mengumpulkan bukti dari berbagai sumber data. Dalam setiap penilaian, Anda menentukan Manajer Akun AWS Audit mana yang akan mengumpulkan bukti, dan Manajer Audit mengelola mana yang Layanan AWS berada dalam ruang lingkup. Masing-masing layanan dan akun ini berisi beberapa sumber daya yang Anda miliki dan gunakan. Pengumpulan bukti di Audit Manager melibatkan penilaian setiap sumber daya dalam lingkup. Ini disebut sebagai penilaian sumber daya.

Langkah-langkah berikut menjelaskan bagaimana Manajer Audit mengumpulkan bukti untuk setiap penilaian sumber daya:

1. Menilai sumber daya dari sumber data

Untuk memulai pengumpulan bukti, Manajer Audit menilai sumber daya dalam lingkup dari sumber data. Ini dilakukan dengan mengambil snapshot konfigurasi, hasil pemeriksaan kepatuhan terkait, atau aktivitas pengguna. Kemudian menjalankan analisis untuk menentukan kontrol mana yang didukung data ini. Hasil penilaian sumber daya kemudian disimpan dan diubah menjadi bukti. Untuk informasi lebih lanjut tentang berbagai jenis bukti, lihat [evidence](#) di bagian AWS Audit Manager konsep dan terminologi panduan ini.

2. Mengkonversi hasil penilaian menjadi bukti

Hasil penilaian sumber daya berisi data asli yang diambil dari sumber daya tersebut, dan metadata yang menunjukkan kontrol mana yang didukung data. Audit Manager mengonversi data asli ke dalam format yang ramah auditor. Data dan metadata yang dikonversi kemudian disimpan sebagai bukti Manajer Audit sebelum dilampirkan ke kontrol.

3. Melampirkan bukti ke kontrol terkait

Manajer Audit membaca metadata bukti. Kemudian, ia melampirkan bukti yang disimpan ke kontrol terkait dalam penilaian. Bukti terlampir menjadi terlihat di Manajer Audit. Ini melengkapi siklus penilaian sumber daya.

Note

Bergantung pada konfigurasi kontrol, bukti yang sama dapat, dalam beberapa kasus, dilampirkan ke beberapa kontrol dari beberapa penilaian Manajer Audit. Ketika bukti yang sama dilampirkan ke beberapa kontrol, Manajer Audit mengukur penilaian sumber daya tepat sekali. Ini karena bukti yang sama dikumpulkan hanya sekali. Namun, satu kontrol dalam penilaian Manajer Audit dapat memiliki beberapa bukti dari berbagai sumber data.

Frekuensi pengumpulan bukti

Pengumpulan bukti adalah proses berkelanjutan yang dimulai ketika Anda membuat penilaian Anda. Manajer Audit mengumpulkan bukti dari berbagai sumber data pada frekuensi yang berbeda-beda. Akibatnya, tidak ada jawaban yang cocok untuk semua tentang seberapa sering bukti dikumpulkan. Frekuensi pengumpulan bukti didasarkan pada jenis bukti dan sumber datanya, seperti yang dijelaskan di bawah ini.

- **Pemeriksaan kepatuhan** — Manajer Audit mengumpulkan jenis bukti ini dari AWS Security Hub CSPM dan AWS Config.
 - Untuk Security Hub CSPM, pengumpulan bukti mengikuti jadwal pemeriksaan CSPM Security Hub Anda. Untuk informasi selengkapnya tentang jadwal pemeriksaan CSPM Security Hub, lihat [Jadwal menjalankan pemeriksaan keamanan](#) di Panduan AWS Security Hub CSPM Pengguna. Untuk informasi selengkapnya tentang pemeriksaan CSPM Security Hub yang didukung oleh Audit Manager, lihat [AWS Security Hub CSPM kontrol didukung oleh AWS Audit Manager](#).
 - Karena AWS Config, pengumpulan bukti mengikuti pemicu yang ditentukan dalam AWS Config aturan Anda. Untuk informasi selengkapnya tentang pemicu AWS Config aturan, lihat [Jenis pemicu](#) di Panduan AWS Config Pengguna. Untuk informasi selengkapnya tentang Aturan AWS Config yang didukung oleh Audit Manager, lihat [Aturan AWS Config didukung oleh AWS Audit Manager](#).
- AWS Audit Manager Menandai bukti sebagai tidak meyakinkan ketika evaluasi kepatuhan otomatis tidak memungkinkan. Ini terjadi ketika Anda belum mengaktifkan AWS Config atau AWS Security Hub CSPM, yang merupakan sumber data utama. Ini juga terjadi ketika bukti dikumpulkan langsung dari AWS layanan melalui panggilan API, AWS CloudTrail log, atau

unggahan manual. Ketika tidak ada mekanisme untuk evaluasi otomatis bukti ini, tidak AWS Audit Manager dapat memberikan rincian evaluasi. Akibatnya, itu menandai bukti sebagai tidak meyakinkan. Bukti yang tidak meyakinkan tidak menunjukkan kegagalan. Sebaliknya, ini menandakan bahwa Anda perlu mengevaluasi bukti kepatuhan secara manual.

- **Aktivitas pengguna** — Manajer Audit mengumpulkan jenis bukti ini AWS CloudTrail secara terus-menerus. Frekuensi ini terus menerus karena aktivitas pengguna dapat terjadi kapan saja sepanjang hari. Untuk informasi selengkapnya, lihat [AWS CloudTrail nama acara didukung oleh AWS Audit Manager](#).
- **Data konfigurasi** — Audit Manager mengumpulkan jenis bukti ini menggunakan panggilan API deskripsi ke yang lain Layanan AWS seperti Amazon EC2, Amazon S3, atau IAM. Anda dapat memilih tindakan API mana yang akan dipanggil. Anda juga mengatur frekuensi sebagai harian, mingguan, atau bulanan di Manajer Audit. Anda dapat menentukan frekuensi ini saat Anda membuat atau mengedit kontrol di pustaka kontrol. Untuk petunjuk tentang cara mengedit atau membuat kontrol, lihat [Menggunakan pustaka kontrol untuk mengelola kontrol di AWS Audit Manager](#). Untuk informasi selengkapnya tentang panggilan API yang didukung oleh Audit Manager, lihat [AWS Panggilan API didukung oleh AWS Audit Manager](#).

Terlepas dari frekuensi pengumpulan bukti untuk sumber data, bukti baru dikumpulkan secara otomatis selama kontrol dan penilaian aktif.

Contoh AWS Audit Manager mengendalikan

Anda dapat meninjau contoh di halaman ini untuk mempelajari lebih lanjut tentang cara kerja kontrol AWS Audit Manager.

Di Audit Manager, kontrol dapat secara otomatis mengumpulkan bukti dari empat jenis sumber data:

1. **AWS CloudTrail**— Tangkap aktivitas pengguna dari CloudTrail log Anda dan impor sebagai bukti aktivitas pengguna
2. **AWS Security Hub CSPM**— Kumpulkan temuan dari Security Hub CSPM dan impor sebagai bukti pemeriksaan kepatuhan
3. **AWS Config**— Kumpulkan evaluasi aturan dari AWS Config dan impor sebagai bukti pemeriksaan kepatuhan
4. **AWS Panggilan API** — Ambil snapshot sumber daya dari panggilan API dan impor sebagai bukti data konfigurasi

Perhatikan bahwa beberapa kontrol mengumpulkan bukti menggunakan pengelompokan yang telah ditentukan dari sumber data ini. Pengelompokan sumber data ini dikenal sebagai sumber [ter](#) AWS kelola. Setiap AWS sumber terkelola mewakili kontrol umum atau kontrol inti. Sumber terkelola ini memberi Anda cara yang efisien untuk memetakan persyaratan kepatuhan Anda ke kelompok sumber data mendasar yang relevan yang divalidasi dan dikelola oleh penilai bersertifikat [industri](#) di AWS.

Contoh di halaman ini menunjukkan bagaimana kontrol mengumpulkan bukti dari masing-masing jenis sumber data individu. Mereka menjelaskan seperti apa kontrol, bagaimana Audit Manager mengumpulkan bukti dari sumber data, dan langkah selanjutnya yang dapat Anda ambil untuk menunjukkan kepatuhan.

Tip

Kami menyarankan Anda mengaktifkan AWS Config dan Security Hub CSPM untuk pengalaman optimal di Audit Manager. Saat Anda mengaktifkan layanan ini, Audit Manager dapat menggunakan temuan Security Hub CSPM dan Aturan AWS Config menghasilkan bukti otomatis.

- Setelah Anda [mengaktifkan AWS Security Hub CSPM](#), pastikan Anda juga [mengaktifkan semua standar keamanan](#) dan [mengaktifkan pengaturan temuan kontrol konsolidasi](#). Langkah ini memastikan bahwa Audit Manager dapat mengimpor temuan untuk semua standar kepatuhan yang didukung.
- Setelah Anda [mengaktifkan AWS Config](#), pastikan Anda juga [mengaktifkan paket kesesuaian yang relevan Aturan AWS Config](#) atau [menerapkan paket kesesuaian](#) untuk standar kepatuhan yang terkait dengan audit Anda. Langkah ini memastikan bahwa Audit Manager dapat mengimpor temuan untuk semua yang didukung Aturan AWS Config yang Anda aktifkan.

Contoh tersedia untuk masing-masing jenis kontrol berikut:

Topik

- [Kontrol otomatis yang menggunakan AWS Security Hub CSPM sebagai tipe sumber data](#)
- [Kontrol otomatis yang menggunakan AWS Config sebagai tipe sumber data](#)
- [Kontrol otomatis yang menggunakan AWS Panggilan API sebagai tipe sumber data](#)
- [Kontrol otomatis yang menggunakan AWS CloudTrail sebagai tipe sumber data](#)

- [Kontrol manual](#)
- [Kontrol dengan tipe sumber data campuran \(otomatis dan manual\)](#)

Kontrol otomatis yang menggunakan AWS Security Hub CSPM sebagai tipe sumber data

Contoh ini menunjukkan kontrol yang digunakan AWS Security Hub CSPM sebagai tipe sumber data. Ini adalah kontrol standar yang diambil dari kerangka F [AWS oundational Security Best Practices \(FSBP\)](#). Audit Manager menggunakan kontrol ini untuk menghasilkan bukti yang dapat membantu menyesuaikan AWS lingkungan Anda dengan persyaratan FSBP.

Contoh detail kontrol

- Nama kontrol — FSBP1-012: AWS Config should be enabled
- Set kontrol — Config. Ini adalah pengelompokan khusus kerangka kerja kontrol FSBP yang berhubungan dengan manajemen konfigurasi.
- Sumber bukti — Sumber data individu
- Jenis sumber data - AWS Security Hub CSPM
- Jenis bukti — Pemeriksaan kepatuhan

Dalam contoh berikut, kontrol ini muncul dalam penilaian Manajer Audit yang dibuat dari kerangka kerja FSBP.

Control sets (32) Delegate control set Complete control set review

Q AWS Config should be enabled X

Controls grouped by control set	Control status	Delegated to	Total evidence
☐ ☒ Config (1)	Active	-	0
☐ FSBP1-012: AWS Config should be enabled	Under review	-	0

Penilaian menunjukkan status kontrol. Ini juga menunjukkan berapa banyak bukti yang dikumpulkan untuk kontrol ini sejauh ini. Dari sini, Anda dapat mendelegasikan kumpulan kontrol untuk ditinjau atau menyelesaikan peninjauan sendiri. Memilih nama kontrol membuka halaman detail dengan informasi lebih lanjut, termasuk bukti untuk kontrol itu.

Apa yang dilakukan kontrol ini

Kontrol ini mengharuskan itu AWS Config diaktifkan di semua Wilayah AWS tempat Anda menggunakan Security Hub CSPM. Audit Manager dapat menggunakan kontrol ini untuk memeriksa apakah Anda telah mengaktifkan AWS Config.

Bagaimana Manajer Audit mengumpulkan bukti untuk kontrol ini

Manajer Audit mengambil langkah-langkah berikut untuk mengumpulkan bukti untuk kontrol ini:

1. Untuk setiap kontrol, Audit Manager menilai sumber daya dalam lingkup Anda. Hal ini dilakukan dengan menggunakan sumber data yang ditentukan dalam pengaturan kontrol. Dalam contoh ini, AWS Config pengaturan Anda adalah sumber daya, dan Security Hub CSPM adalah jenis sumber data. Audit Manager mencari hasil pemeriksaan CSPM Security Hub tertentu ([\[Config.1\]](#)).
2. Hasil penilaian sumber daya disimpan dan diubah menjadi bukti yang ramah auditor. Audit Manager menghasilkan bukti pemeriksaan kepatuhan untuk kontrol yang menggunakan Security Hub CSPM sebagai jenis sumber data. Bukti ini berisi hasil pemeriksaan kepatuhan yang dilaporkan langsung dari Security Hub CSPM.
3. Manajer Audit melampirkan bukti yang disimpan ke kontrol dalam penilaian Anda yang diberi namaFSBP1-012: AWS Config should be enabled.

Bagaimana Anda dapat menggunakan Audit Manager untuk menunjukkan kepatuhan terhadap kontrol ini

Setelah bukti dilampirkan pada kontrol, Anda—atau delegasi pilihan Anda—dapat meninjau bukti untuk melihat apakah ada perbaikan yang diperlukan.

Dalam contoh ini, Audit Manager mungkin menampilkan put usan Gagal dari Security Hub CSPM. Ini dapat terjadi jika Anda belum mengaktifkan AWS Config. Dalam hal ini, Anda dapat mengambil tindakan korektif untuk mengaktifkan AWS Config, yang membantu menyesuaikan AWS lingkungan Anda dengan persyaratan FSBP.

Ketika AWS Config pengaturan Anda sejalan dengan kontrol, tandai kontrol sebagai T injau dan tambahkan bukti ke laporan penilaian Anda. Anda kemudian dapat membagikan laporan ini dengan auditor untuk menunjukkan bahwa kontrol berfungsi sebagaimana dimaksud.

Kontrol otomatis yang menggunakan AWS Config sebagai tipe sumber data

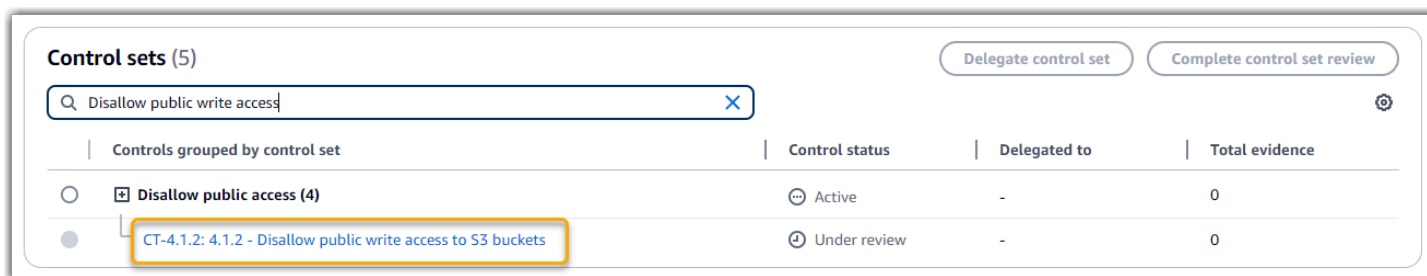
Contoh ini menunjukkan kontrol yang digunakan AWS Config sebagai tipe sumber data. Ini adalah kontrol standar yang diambil dari kerangka [AWS Control Tower Guardrails](#). Audit Manager

menggunakan kontrol ini untuk menghasilkan bukti yang membantu menyelaraskan AWS lingkungan Anda dengan AWS Control Tower Guardrails.

Contoh detail kontrol

- Nama kontrol — CT-4.1.2: 4.1.2 - Disallow public write access to S3 buckets
- Kumpulan kontrol — Kontrol ini milik kumpulan Disallow public access pulan kontrol. Ini adalah pengelompokan kontrol yang berhubungan dengan manajemen akses.
- Sumber bukti — Sumber data individu
- Jenis sumber data - AWS Config
- Jenis bukti — Pemeriksaan kepatuhan

Dalam contoh berikut, kontrol ini muncul dalam penilaian Manajer Audit yang dibuat dari kerangka kerja AWS Control Tower Guardrails.



Controls grouped by control set	Control status	Delegated to	Total evidence
○ [x] Disallow public access (4)	☑ Active	-	0
● CT-4.1.2: 4.1.2 - Disallow public write access to S3 buckets	⌚ Under review	-	0

Penilaian menunjukkan status kontrol. Ini juga menunjukkan berapa banyak bukti yang dikumpulkan untuk kontrol ini sejauh ini. Dari sini, Anda dapat mendelegasikan kumpulan kontrol untuk ditinjau atau menyelesaikan peninjauan sendiri. Memilih nama kontrol membuka halaman detail dengan informasi lebih lanjut, termasuk bukti untuk kontrol itu.

Apa yang dilakukan kontrol ini

Audit Manager dapat menggunakan kontrol ini untuk memeriksa apakah tingkat akses kebijakan bucket S3 Anda terlalu lunak untuk memenuhi AWS Control Tower persyaratan. Lebih khusus lagi, dapat memeriksa pengaturan Blokir Akses Publik, kebijakan bucket, dan daftar kontrol akses bucket (ACL) untuk mengonfirmasi bahwa bucket Anda tidak mengizinkan akses tulis publik.

Bagaimana Manajer Audit mengumpulkan bukti untuk kontrol ini

Manajer Audit mengambil langkah-langkah berikut untuk mengumpulkan bukti untuk kontrol ini:

1. Untuk setiap kontrol, Audit Manager menilai sumber daya dalam lingkup Anda menggunakan sumber data yang ditentukan dalam pengaturan kontrol. Dalam hal ini, bucket S3 Anda adalah sumber daya, dan AWS Config merupakan jenis sumber data. Audit Manager mencari hasil dari A AWS Config turan tertentu ([s3-bucket-public-write-](#)) untuk mengevaluasi pengaturan, kebijakan, dan ACL dari masing-masing bucket S3 yang berada dalam lingkup penilaian Anda.
2. Hasil penilaian sumber daya disimpan dan diubah menjadi bukti yang ramah auditor. Audit Manager menghasilkan bukti pemeriksaan kepatuhan untuk kontrol yang digunakan AWS Config sebagai jenis sumber data. Bukti ini berisi hasil pemeriksaan kepatuhan yang dilaporkan langsung dari AWS Config.
3. Manajer Audit melampirkan bukti yang disimpan ke kontrol dalam penilaian Anda yang diberi nama CT-4.1.2: 4.1.2 - Disallow public write access to S3 buckets.

Bagaimana Anda dapat menggunakan Audit Manager untuk menunjukkan kepatuhan terhadap kontrol ini

Setelah bukti dilampirkan pada kontrol, Anda—atau delegasi pilihan Anda—dapat meninjau bukti untuk melihat apakah ada perbaikan yang diperlukan.

Dalam contoh ini, Audit Manager mungkin menampilkan aturan dari AWS Config menyatakan bahwa bucket S3 tidak sesuai. Hal ini dapat terjadi jika salah satu bucket S3 Anda memiliki setelan Blokir Akses Publik yang tidak membatasi kebijakan publik, dan kebijakan yang digunakan mengizinkan akses penulisan publik. Untuk memperbaiki ini, Anda dapat memperbarui setelan Blokir Akses Publik untuk membatasi kebijakan publik. Atau, Anda dapat menggunakan kebijakan bucket berbeda yang tidak mengizinkan akses penulisan publik. Tindakan korektif ini membantu AWS menyesuaikan lingkungan Anda dengan AWS Control Tower persyaratan.

Ketika Anda puas bahwa tingkat akses bucket S3 Anda sejalan dengan kontrol, Anda dapat menandai kontrol sebagai Tinjau dan menambahkan bukti ke laporan penilaian Anda. Anda kemudian dapat membagikan laporan ini dengan auditor untuk menunjukkan bahwa kontrol berfungsi sebagaimana dimaksud.

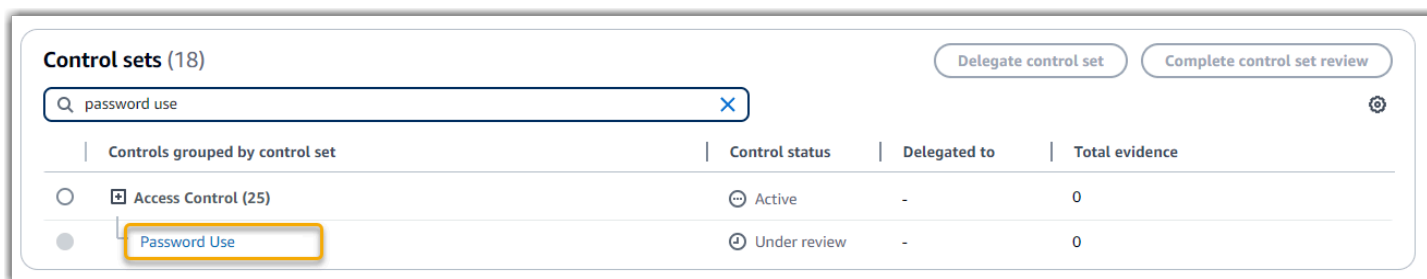
Kontrol otomatis yang menggunakan AWS Panggilan API sebagai tipe sumber data

Contoh ini menunjukkan kontrol kustom yang menggunakan panggilan AWS API sebagai tipe sumber data. Audit Manager menggunakan kontrol ini untuk menghasilkan bukti yang dapat membantu menyesuaikan AWS lingkungan Anda dengan persyaratan spesifik Anda.

Contoh detail kontrol

- Nama kontrol — Password Use
- Kumpulan kontrol — Kontrol ini milik kumpulan kontrol yang dipanggil `Access Control`. Ini adalah pengelompokan kontrol yang berhubungan dengan identitas dan manajemen akses.
- Sumber bukti — Sumber data individu
- Jenis sumber data — Panggilan AWS API
- Jenis bukti — Data konfigurasi

Dalam contoh berikut, kontrol ini muncul dalam penilaian Manajer Audit yang dibuat dari kerangka kerja khusus.



Penilaian menunjukkan status kontrol. Ini juga menunjukkan berapa banyak bukti yang dikumpulkan untuk kontrol ini sejauh ini. Dari sini, Anda dapat mendelegasikan kumpulan kontrol untuk ditinjau atau menyelesaikan peninjauan sendiri. Memilih nama kontrol membuka halaman detail dengan informasi lebih lanjut, termasuk bukti untuk kontrol itu.

Apa yang dilakukan kontrol ini

Audit Manager dapat menggunakan kontrol khusus ini untuk membantu Anda memastikan bahwa Anda memiliki kebijakan kontrol akses yang memadai. Kontrol ini mengharuskan Anda mengikuti praktik keamanan yang baik dalam pemilihan dan penggunaan kata sandi. Audit Manager dapat membantu Anda memvalidasi ini dengan mengambil daftar semua kebijakan kata sandi untuk prinsipal IAM yang berada dalam lingkup penilaian Anda.

Bagaimana Manajer Audit mengumpulkan bukti untuk kontrol ini

Audit Manager mengambil langkah-langkah berikut untuk mengumpulkan bukti untuk kontrol kustom ini:

1. Untuk setiap kontrol, Audit Manager menilai sumber daya dalam lingkup Anda menggunakan sumber data yang ditentukan dalam pengaturan kontrol. Dalam hal ini, prinsipal IAM Anda adalah

- sumber daya, dan panggilan AWS API adalah jenis sumber data. Audit Manager mencari respons panggilan IAM API tertentu ([GetAccountPasswordPolicy](#)). Kemudian mengembalikan kebijakan kata sandi untuk Akun AWS yang berada dalam lingkup penilaian Anda.
2. Hasil penilaian sumber daya disimpan dan diubah menjadi bukti yang ramah auditor. Audit Manager menghasilkan bukti data konfigurasi untuk kontrol yang menggunakan panggilan API sebagai sumber data. Bukti ini berisi data asli yang diambil dari respons API, dan metadata tambahan yang menunjukkan kontrol mana yang didukung data.
 3. Audit Manager melampirkan bukti yang disimpan ke kontrol kustom dalam penilaian Anda yang diberi nama `Password Use`.

Bagaimana Anda dapat menggunakan Audit Manager untuk menunjukkan kepatuhan terhadap kontrol ini

Setelah bukti dilampirkan pada kontrol, Anda—atau delegasi pilihan Anda—dapat meninjau bukti untuk melihat apakah itu cukup atau apakah ada perbaikan yang diperlukan.

Dalam contoh ini, Anda dapat meninjau bukti untuk melihat respons dari panggilan API. Tanggapan [GetAccountPasswordPolicy](#) menjelaskan persyaratan kompleksitas dan periode rotasi wajib untuk kata sandi pengguna di akun Anda. Anda dapat menggunakan respons API ini sebagai bukti untuk menunjukkan bahwa Anda memiliki kebijakan kontrol akses kata sandi yang memadai untuk Akun AWS yang berada dalam lingkup penilaian Anda. Jika mau, Anda juga dapat memberikan komentar tambahan tentang kebijakan ini dengan menambahkan komentar ke kontrol.

Ketika Anda puas bahwa kebijakan kata sandi kepala sekolah IAM Anda sejalan dengan kontrol khusus, Anda dapat menandai kontrol sebagai *Tinjau* dan menambahkan bukti ke laporan penilaian Anda. Anda kemudian dapat membagikan laporan ini dengan auditor untuk menunjukkan bahwa kontrol berfungsi sebagaimana dimaksud.

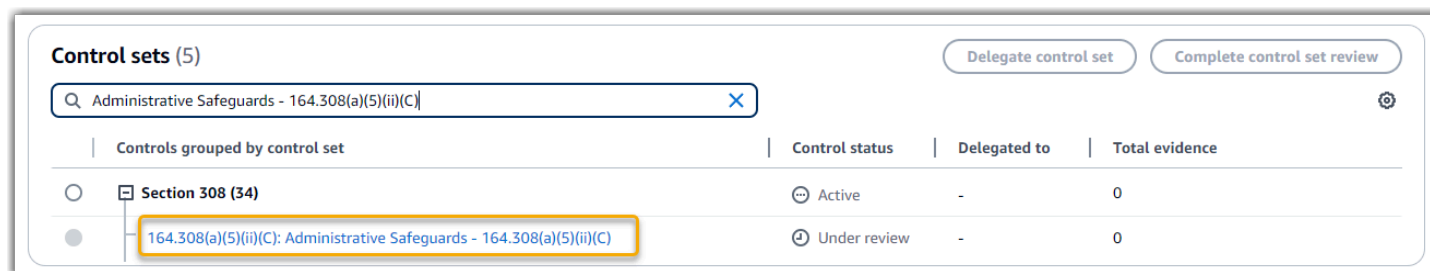
Kontrol otomatis yang menggunakan AWS CloudTrail sebagai tipe sumber data

Contoh ini menunjukkan kontrol yang digunakan AWS CloudTrail sebagai tipe sumber data. Ini adalah kontrol standar yang diambil dari kerangka <https://docs.aws.amazon.com/audit-manager/latest/userguide/HIPAA.html> HIPAA Security Rule 2003. Audit Manager menggunakan kontrol ini untuk menghasilkan bukti yang dapat membantu menyesuaikan AWS lingkungan Anda dengan persyaratan HIPAA.

Contoh detail kontrol

- Nama kontrol — 164.308(a)(5)(ii)(C): Administrative Safeguards - 164.308(a)(5)(ii)(C)
- Kumpulan kontrol — Kontrol ini milik kumpulan kontrol yang dipanggil Section 308. Ini adalah pengelompokan kontrol HIPAA khusus kerangka kerja yang berhubungan dengan pengamanan administratif.
- Sumber bukti — sumber AWS terkelola (kontrol inti)
- Jenis sumber data yang mendasarinya — AWS CloudTrail
- Jenis bukti — Aktivitas pengguna

Berikut kontrol ini ditampilkan dalam penilaian Manajer Audit yang dibuat dari kerangka kerja HIPAA:



Penilaian menunjukkan status kontrol. Ini juga menunjukkan berapa banyak bukti yang dikumpulkan untuk kontrol ini sejauh ini. Dari sini, Anda dapat mendelegasikan kumpulan kontrol untuk ditinjau atau menyelesaikan peninjauan sendiri. Memilih nama kontrol membuka halaman detail dengan informasi lebih lanjut, termasuk bukti untuk kontrol itu.

Apa yang dilakukan kontrol ini

Kontrol ini mengharuskan Anda memiliki prosedur pemantauan untuk mendeteksi akses yang tidak sah. Contoh akses tidak sah adalah ketika seseorang masuk ke konsol tanpa otentikasi multi-faktor (MFA) diaktifkan. Audit Manager membantu Anda memvalidasi kontrol ini dengan memberikan bukti bahwa Anda mengonfigurasi Amazon CloudWatch untuk memantau permintaan masuk konsol manajemen di mana MFA tidak diaktifkan.

Bagaimana Manajer Audit mengumpulkan bukti untuk kontrol ini

Manajer Audit mengambil langkah-langkah berikut untuk mengumpulkan bukti untuk kontrol ini:

1. Untuk setiap kontrol, Audit Manager menilai sumber daya dalam lingkup Anda menggunakan sumber bukti yang ditentukan dalam pengaturan kontrol. Dalam hal ini, kontrol menggunakan beberapa kontrol inti sebagai sumber bukti.

Setiap kontrol inti adalah pengelompokan sumber data individual yang dikelola. Dalam contoh kita, salah satu kontrol inti ini (Configure Amazon CloudWatch alarms to detect management console sign-in requests without MFA enabled) menggunakan CloudTrail event (`monitoring_EnableAlarmActions`) sebagai sumber data yang mendasarinya.

Audit Manager meninjau log CloudTrail Anda, menggunakan `monitoring_EnableAlarmActions` kata kunci untuk menemukan tindakan yang mengaktifkan CloudWatch alarm yang dicatat oleh CloudTrail. Kemudian mengembalikan log peristiwa yang relevan yang berada dalam lingkup penilaian Anda.

2. Hasil penilaian sumber daya disimpan dan diubah menjadi bukti yang ramah auditor. Audit Manager menghasilkan bukti aktivitas pengguna untuk kontrol yang digunakan CloudTrail sebagai jenis sumber data. Bukti ini berisi data asli yang diambil dari Amazon CloudWatch, dan metadata tambahan yang menunjukkan kontrol mana yang didukung data.
3. Manajer Audit melampirkan bukti yang disimpan ke kontrol dalam penilaian Anda yang diberi nama `164.308(a)(5)(ii)(C): Administrative Safeguards - 164.308(a)(5)(ii)(C)`.

Bagaimana Anda dapat menggunakan Audit Manager untuk menunjukkan kepatuhan terhadap kontrol ini

Setelah bukti dilampirkan pada kontrol, Anda—atau delegasi pilihan Anda—dapat meninjau bukti untuk melihat apakah ada perbaikan yang diperlukan.

Dalam contoh ini, Anda dapat meninjau bukti untuk melihat peristiwa pengaktifan alarm yang dicatat oleh CloudTrail Anda dapat menggunakan log ini sebagai bukti untuk menunjukkan bahwa Anda memiliki prosedur pemantauan yang memadai untuk mendeteksi saat masuk konsol terjadi tanpa MFA diaktifkan. Jika Anda suka, Anda juga dapat memberikan komentar tambahan dengan menambahkan komentar ke kontrol. Misalnya, jika log menunjukkan beberapa login tanpa MFA, Anda dapat menambahkan komentar yang menjelaskan cara Anda memperbaiki masalah. Pemantauan masuk konsol secara teratur membantu Anda mencegah masalah keamanan yang mungkin timbul dari perbedaan dan upaya masuk yang tidak pantas. Pada gilirannya, praktik terbaik ini membantu menyesuaikan AWS lingkungan Anda dengan persyaratan HIPAA.

Ketika Anda puas bahwa prosedur pemantauan Anda sejalan dengan kontrol, Anda dapat menandai kontrol sebagai **Tinjau** dan menambahkan bukti ke laporan penilaian Anda. Anda kemudian dapat membagikan laporan ini dengan auditor untuk menunjukkan bahwa kontrol berfungsi sebagaimana dimaksud.

Kontrol manual

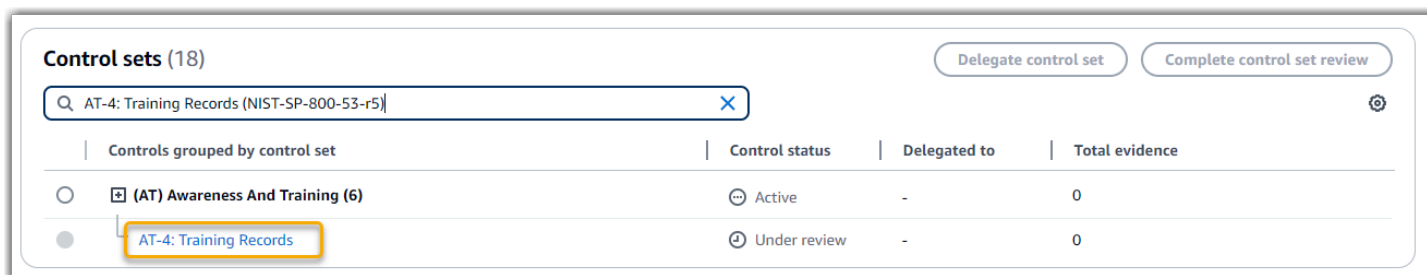
Beberapa kontrol tidak mendukung pengumpulan bukti otomatis. Ini termasuk kontrol yang bergantung pada penyediaan catatan fisik dan tanda tangan, selain pengamatan, wawancara, dan peristiwa lain yang tidak dihasilkan di cloud. Dalam kasus ini, Anda dapat mengunggah bukti secara manual untuk menunjukkan bahwa Anda memenuhi persyaratan kontrol.

Contoh ini menunjukkan kontrol manual yang diambil dari kerangka kerja [NIST 800-53 \(Rev. 5\)](#). Anda dapat menggunakan Audit Manager untuk mengunggah dan menyimpan bukti yang menunjukkan kepatuhan untuk kontrol ini.

Contoh detail kontrol

- Nama kontrol — AT-4: Training Records
- Set kontrol —(AT) Awareness and training. Ini adalah pengelompokan kontrol NIST khusus kerangka kerja yang berhubungan dengan pelatihan.
- Sumber bukti — Sumber data individu
- Jenis sumber data - Manual
- Jenis bukti — Manual

Berikut kontrol yang ditunjukkan dalam penilaian Manajer Audit yang dibuat dari kerangka kerja NIST 800-53 (Rev. 5): Low-Moderate-High



Control sets (18)

Delegate control set Complete control set review

Q AT-4: Training Records (NIST-SP-800-53-r5) X

Controls grouped by control set	Control status	Delegated to	Total evidence
☐ (AT) Awareness And Training (6)	Active	-	0
☒ AT-4: Training Records	Under review	-	0

Penilaian menunjukkan status kontrol. Ini juga menunjukkan berapa banyak bukti yang dikumpulkan untuk kontrol ini sejauh ini. Dari sini, Anda dapat mendelegasikan kumpulan kontrol untuk ditinjau

atau menyelesaikan peninjauan sendiri. Memilih nama kontrol membuka halaman detail dengan informasi lebih lanjut, termasuk bukti untuk kontrol itu.

Apa yang dilakukan kontrol ini

Anda dapat menggunakan kontrol ini untuk membantu memastikan bahwa personel Anda menerima tingkat pelatihan keamanan dan privasi yang sesuai. Secara khusus, Anda dapat menunjukkan bahwa Anda telah mendokumentasikan kegiatan pelatihan keamanan dan privasi untuk semua staf, berdasarkan peran mereka. Anda juga dapat menunjukkan bukti bahwa catatan pelatihan disimpan untuk setiap individu.

Bagaimana Anda dapat mengunggah bukti secara manual untuk kontrol ini

Untuk mengunggah bukti manual yang melengkapi bukti otomatis, lihat Meng [unggah bukti manual di AWS Audit Manager](#). Manajer Audit melampirkan bukti yang diunggah ke kontrol dalam penilaian Anda yang diberi nama AT-4: Training Records.

Bagaimana Anda dapat menggunakan Audit Manager untuk menunjukkan kepatuhan terhadap kontrol ini

Jika Anda memiliki dokumentasi yang mendukung kontrol ini, Anda dapat mengunggahnya sebagai bukti manual. Misalnya, Anda dapat mengunggah salinan terbaru dari materi pelatihan berbasis peran yang diamanatkan yang dikeluarkan departemen Sumber Daya Manusia kepada karyawan.

Sama seperti kontrol otomatis, Anda dapat mendelegasikan kontrol manual kepada pemangku kepentingan yang dapat membantu Anda meninjau bukti (atau, dalam hal ini, menyediakannya). Misalnya, ketika Anda meninjau kontrol ini, Anda mungkin menyadari bahwa Anda hanya memenuhi sebagian persyaratannya. Ini bisa terjadi jika Anda tidak memiliki salinan pelacakan kehadiran untuk pelatihan tatap muka. Anda dapat mendelegasikan kontrol ke pemangku kepentingan SDM, yang kemudian dapat mengunggah daftar staf yang menghadiri pelatihan.

Ketika Anda puas bahwa Anda sejalan dengan kontrol, Anda dapat menandainya sebagai Tinjau dan menambahkan bukti ke laporan penilaian Anda. Anda kemudian dapat membagikan laporan ini dengan auditor untuk menunjukkan bahwa kontrol berfungsi sebagaimana dimaksud.

Kontrol dengan tipe sumber data campuran (otomatis dan manual)

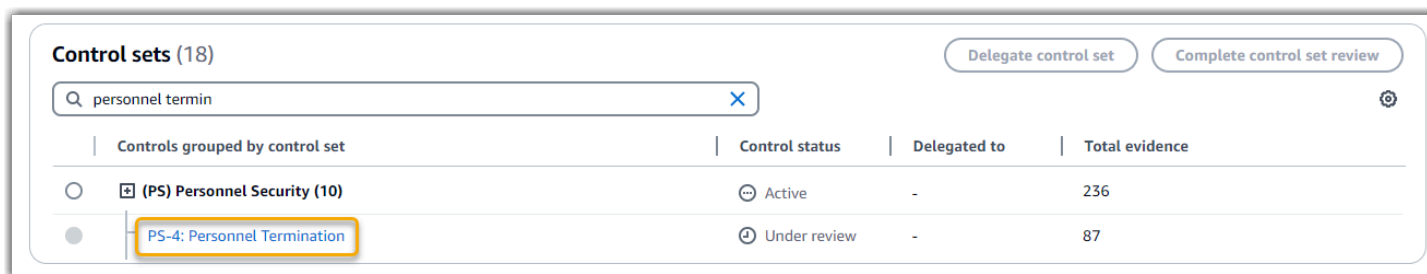
Dalam banyak kasus, kombinasi bukti otomatis dan manual diperlukan untuk memenuhi kontrol. Meskipun Audit Manager dapat memberikan bukti otomatis yang relevan dengan kontrol, Anda mungkin perlu melengkapi data ini dengan bukti manual yang Anda identifikasi dan unggah sendiri.

Contoh ini menunjukkan kontrol yang menggunakan kombinasi bukti manual dan bukti otomatis. Ini adalah kontrol standar yang diambil dari kerangka kerja [NIST 800-53 \(Rev. 5\)](#). Audit Manager menggunakan kontrol ini untuk menghasilkan bukti yang dapat membantu menyesuaikan AWS lingkungan Anda dengan persyaratan NIST.

Contoh detail kontrol

- Nama kontrol — Personnel Termination
- Set kontrol —(PS) Personnel Security (10). Ini adalah pengelompokan kontrol NIST khusus kerangka kerja yang berhubungan dengan individu yang melakukan pemeliharaan perangkat keras atau perangkat lunak pada sistem organisasi.
- Sumber bukti — AWS dikelola (kontrol inti) dan sumber data individu (manual)
- Jenis sumber data yang mendasarinya - panggilan AWS API AWS CloudTrail, AWS Config,, Manual
- Jenis bukti — Data konfigurasi, aktivitas pengguna, pemeriksaan kepatuhan, bukti manual)

Berikut kontrol yang ditunjukkan dalam penilaian Manajer Audit yang dibuat dari kerangka kerja NIST 800-53 (Rev. 5):



Controls grouped by control set	Control status	Delegated to	Total evidence
☐ (PS) Personnel Security (10)	Active	-	236
☒ PS-4: Personnel Termination	Under review	-	87

Penilaian menunjukkan status kontrol. Ini juga menunjukkan berapa banyak bukti yang dikumpulkan untuk kontrol ini sejauh ini. Dari sini, Anda dapat mendelegasikan kumpulan kontrol untuk ditinjau atau menyelesaikan peninjauan sendiri. Memilih nama kontrol membuka halaman detail dengan informasi lebih lanjut, termasuk bukti untuk kontrol itu.

Apa yang dilakukan kontrol ini

Anda dapat menggunakan kontrol ini untuk mengonfirmasi bahwa Anda melindungi informasi organisasi jika karyawan diberhentikan. Secara khusus, Anda dapat menunjukkan bahwa Anda menonaktifkan akses sistem dan mencabut kredensial untuk individu tersebut. Selain itu, Anda dapat menunjukkan bahwa semua orang yang diberhentikan berpartisipasi dalam wawancara keluar yang mencakup diskusi tentang protokol keamanan yang relevan untuk organisasi Anda.

Bagaimana Manajer Audit mengumpulkan bukti untuk kontrol ini

Manajer Audit mengambil langkah-langkah berikut untuk mengumpulkan bukti untuk kontrol ini:

1. Untuk setiap kontrol, Audit Manager menilai sumber daya dalam lingkup Anda menggunakan sumber bukti yang ditentukan dalam pengaturan kontrol.

Dalam hal ini, kontrol menggunakan beberapa kontrol inti sebagai sumber bukti. Pada gilirannya, masing-masing kontrol inti ini mengumpulkan bukti yang relevan dari sumber data individu (panggilan AWS API, AWS CloudTrail, dan AWS Config). Audit Manager menggunakan jenis sumber data ini untuk menilai sumber daya IAM Anda (seperti grup, kunci, dan kebijakan) terhadap panggilan, CloudTrail peristiwa, dan AWS Config aturan API yang relevan.

2. Hasil penilaian sumber daya disimpan dan diubah menjadi bukti yang ramah auditor. Bukti ini berisi data asli yang diambil dari setiap sumber data, dan metadata tambahan yang menunjukkan kontrol mana yang didukung data.
3. Manajer Audit melampirkan bukti yang disimpan ke kontrol dalam penilaian Anda yang diberi nama `Personnel Termination`.

Bagaimana Anda dapat mengunggah bukti secara manual untuk kontrol ini

Untuk mengunggah bukti manual yang melengkapi bukti otomatis, lihat Meng [unggah bukti manual di AWS Audit Manager](#). Manajer Audit melampirkan bukti yang diunggah ke kontrol dalam penilaian Anda yang diberi nama `Personnel Termination`.

Bagaimana Anda dapat menggunakan Audit Manager untuk menunjukkan kepatuhan terhadap kontrol ini

Setelah bukti dilampirkan pada kontrol, Anda—atau delegasi pilihan Anda—dapat meninjau bukti untuk melihat apakah itu cukup atau apakah ada perbaikan yang diperlukan. Misalnya, ketika Anda meninjau kontrol ini, Anda mungkin menyadari bahwa Anda hanya memenuhi sebagian persyaratannya. Ini bisa terjadi jika Anda memiliki bukti bahwa akses dicabut, tetapi tidak memiliki salinan wawancara keluar apa pun. Anda dapat mendelegasikan kontrol kepada pemangku kepentingan SDM, yang kemudian dapat mengunggah salinan dokumen wawancara keluar. Atau, jika tidak ada karyawan yang diberhentikan selama periode audit, Anda dapat meninggalkan komentar yang menyatakan mengapa tidak ada dokumen yang ditandatangani yang dilampirkan pada kontrol.

Ketika Anda puas bahwa Anda sejalan dengan kontrol, tandai kontrol sebagai Tinjau dan tambahkan bukti ke laporan penilaian Anda. Anda kemudian dapat membagikan laporan ini dengan auditor untuk menunjukkan bahwa kontrol berfungsi sebagaimana dimaksud.

Penggunaan AWS Audit Manager

Anda dapat mengakses AWS Audit Manager melalui berbagai opsi, tergantung pada kebutuhan dan preferensi spesifik Anda. Berikut adalah beberapa cara berbeda Anda dapat berinteraksi dengan Audit Manager:

- Konsol Manajer Audit

Akses konsol Audit Manager langsung di <https://console.aws.amazon.com/auditmanager/home>, yang menyediakan antarmuka yang ramah pengguna untuk mengelola audit Anda dan sumber daya terkait.

- API Manajer Audit

Berinteraksi dengan Audit Manager secara terprogram melalui Audit Manager API, memungkinkan Anda untuk mengotomatiskan dan mengintegrasikan tugas ke dalam alur kerja yang ada. Untuk informasi lebih lanjut, lihat [Referensi API AWS Audit Manager](#).

- AWS SDK

Gunakan AWS perangkat pengembangan perangkat lunak (SDK) untuk berinteraksi dengan Audit Manager secara terprogram, memungkinkan Anda menulis kode dalam berbagai bahasa pemrograman. Untuk informasi selengkapnya, lihat [Penggunaan AWS Audit Manager dengan AWS SDK](#).

- AWS CloudFormation

Buat sumber daya Audit Manager menggunakan AWS CloudFormation, yang memungkinkan Anda untuk menentukan dan menerapkan infrastruktur audit Anda sebagai kode. Untuk informasi selengkapnya, lihat [Membuat sumber daya AWS Audit Manager dengan AWS CloudFormation](#).

- Third-party integrasi

Integrasikan Audit Manager dengan produk Tata Kelola, Risiko, dan Kepatuhan (GRC) pihak ketiga yang didukung, memungkinkan Anda memanfaatkan alat dan proses GRC yang ada. Untuk informasi selengkapnya, lihat [Integrasi dengan produk GRC pihak ketiga](#).

- Integrasi dengan sistem GRC Anda sendiri

Masukkan bukti Manajer Audit ke dalam sistem GRC Anda sendiri, memungkinkan Anda mengirim bukti langsung dari Manajer Audit ke dalam aplikasi GRC Anda. Untuk informasi selengkapnya, lihat [Mengintegrasikan bukti Audit Manager ke dalam sistem GRC Anda](#).

Penggunaan AWS Audit Manager dengan AWS SDK

AWS perangkat pengembangan perangkat lunak (SDK) tersedia untuk banyak bahasa pemrograman populer. Setiap SDK menyediakan API, contoh kode, dan dokumentasi yang dapat digunakan pengembang untuk membangun aplikasi dalam bahasa pilihan mereka.

Dokumentasi SDK	Dokumentasi khusus Manajer Audit	Contoh kode	
AWS SDK untuk C++	AWS SDK untuk C++ Referensi API untuk Audit Manager	AWS SDK untuk C++ contoh kode	
AWS SDK untuk Go	AWS SDK untuk Go Referensi API untuk Audit Manager	AWS SDK untuk Go contoh kode	
AWS SDK untuk Java	AWS SDK for Java 2.x Referensi API untuk Audit Manager	AWS SDK untuk Java contoh kode	
AWS SDK untuk JavaScript	AWS SDK untuk JavaScript Referensi API untuk Audit Manager	AWS SDK untuk JavaScript contoh kode	
AWS SDK untuk .NET	AWS SDK untuk .NET Referensi API untuk Audit Manager	AWS SDK untuk .NET contoh kode	
AWS SDK untuk PHP	AWS SDK untuk PHP Referensi API untuk Audit Manager	AWS SDK untuk PHP contoh kode	
AWS SDK untuk Python (Boto3)	AWS SDK for Python (Boto3) Referensi API untuk Audit Manager	AWS SDK untuk Python (Boto3) contoh kode	

Dokumentasi SDK	Dokumentasi khusus Manajer Audit	Contoh kode	
AWS SDK untuk Ruby	AWS SDK untuk Ruby Referensi API untuk Audit Manager	AWS SDK untuk Ruby contoh kode	

Untuk contoh yang khusus untuk Manajer Audit, lihat Contoh [kode untuk Manajer Audit menggunakan AWS SDK](#).

Note

Audit Manager tersedia di botocore versi 1.19.32 dan yang lebih baru untuk. AWS SDK untuk Python (Boto3) Sebelum Anda mulai menggunakan SDK, pastikan Anda menggunakan versi botocore yang sesuai.

Membuat sumber daya AWS Audit Manager dengan AWS CloudFormation

AWS Audit Manager terintegrasi dengan AWS CloudFormation, layanan yang membantu Anda memodelkan dan mengatur AWS sumber daya sehingga Anda dapat menghabiskan lebih sedikit waktu untuk membuat dan mengelola sumber daya dan infrastruktur Anda. Anda membuat template yang menjelaskan semua AWS sumber daya yang Anda inginkan (seperti penilaian), dan CloudFormation menyediakan serta mengonfigurasi sumber daya tersebut untuk Anda.

Saat menggunakan CloudFormation, Anda dapat menggunakan kembali template untuk mengatur sumber daya AWS Audit Manager secara konsisten dan berulang kali. Jelaskan sumber daya Anda sekali, lalu sediakan sumber daya yang sama berulang-ulang di beberapa AWS akun dan Wilayah.

Manajer Audit AWS dan CloudFormation templat

Untuk menyediakan dan mengonfigurasi sumber daya untuk AWS Audit Manager dan layanan terkait, Anda harus memahami [CloudFormation template](#). Templat adalah file teks dengan format JSON atau YAML. Template ini menjelaskan sumber daya yang ingin Anda sediakan di tumpukan CloudFormation Anda. Jika Anda tidak terbiasa dengan JSON atau YAML, Anda dapat menggunakan CloudFormation Designer untuk membantu Anda memulai dengan CloudFormation template. Untuk informasi selengkapnya, lihat [Apa itu CloudFormation Designer?](#) di Panduan Pengguna AWS CloudFormation .

AWS Audit Manager mendukung pembuatan penilaian di CloudFormation. Untuk informasi selengkapnya, termasuk contoh template JSON dan YAML untuk penilaian, lihat referensi jenis [AWS Audit Manager sumber daya](#) di Panduan AWS CloudFormation Pengguna.

Pelajari lebih lanjut tentang CloudFormation

Untuk mempelajari selengkapnya CloudFormation nya, lihat sumber daya berikut:

- [AWS CloudFormation](#)
- [AWS CloudFormation Panduan Pengguna](#)
- [CloudFormation Referensi API](#)
- [AWS CloudFormation Panduan Pengguna Antarmuka Baris Perintah](#)

Integrasi dengan produk GRC pihak ketiga

AWS Audit Manager mendukung integrasi dengan produk GRC mitra pihak ketiga yang tercantum di halaman ini.

Jika perusahaan Anda menggunakan model cloud hybrid atau model multicloud, kemungkinan Anda menggunakan produk GRC untuk mengelola bukti dari lingkungan tersebut. Ketika produk itu terintegrasi dengan Audit Manager, Anda dapat menarik bukti tentang AWS penggunaan Anda langsung ke lingkungan GRC Anda. Ini menyederhanakan cara Anda mengelola kepatuhan dengan menyediakan tempat terpusat untuk meninjau dan memperbaiki bukti saat Anda mempersiapkan audit.

Baca halaman ini untuk ikhtisar produk GRC pihak ketiga yang dapat menelan bukti dari Manajer Audit. Anda juga dapat melihat referensi tindakan API Manajer Audit mana yang dapat Anda lakukan langsung dalam produk tersebut.

Topik

- [Memahami cara kerja integrasi pihak ketiga dengan Audit Manager](#)
- [Third-party Produk mitra GRC yang terintegrasi dengan Audit Manager](#)

Memahami cara kerja integrasi pihak ketiga dengan Audit Manager

Mitra GRC dapat menggunakan API publik Audit Manager untuk mengintegrasikan produk mereka dengan Audit Manager. Dengan integrasi ini, Anda dapat memetakan kontrol perusahaan di lingkungan GRC Anda ke kontrol umum yang disediakan Audit Manager.

Tip

Anda dapat memetakan kontrol perusahaan Anda ke semua jenis kontrol Manajer [Audit](#). Namun, kami menyarankan Anda menggunakan kontrol umum. Saat Anda memetakan ke kontrol umum yang mewakili tujuan Anda, Audit Manager mengumpulkan bukti dari kelompok sumber data yang telah ditentukan sebelumnya yang dikelola oleh AWS. Ini berarti bahwa Anda tidak harus menjadi AWS ahli untuk mengetahui sumber data mana yang mengumpulkan bukti yang relevan untuk tujuan Anda.

Setelah menyelesaikan latihan pemetaan kontrol satu kali ini, Anda dapat membuat penilaian Manajer Audit langsung di produk GRC. Tindakan ini memulai pengumpulan bukti tentang AWS penggunaan Anda. Anda kemudian dapat melihat AWS bukti ini bersama dengan bukti lain yang dikumpulkan dari lingkungan hibrida Anda, semuanya dalam konteks yang sama dari kontrol perusahaan Anda.

Saat Anda menggunakan integrasi Audit Manager dengan produk GRC pihak ketiga, ingatlah hal-hal berikut:

- Integrasi tersedia untuk semua [Wilayah AWS tempat Audit Manager didukung](#).
- Setiap sumber daya Audit Manager yang Anda buat di produk mitra GRC juga tercermin dalam Manajer Audit.
- Anda tunduk [pada](#) AWS Audit Manager harga selain harga produk GRC pihak ketiga.
- Bukti yang dikumpulkan oleh Manajer Audit tidak dapat diubah. Bukti disajikan dengan cara yang persis sama dalam produk GRC pihak ketiga seperti di konsol Audit Manager. Namun, jika Anda menggunakan integrasi pihak ketiga, Anda mungkin dapat meningkatkan bukti ini dengan memberikan konteks tambahan dalam pelaporan Anda.
- Kuota [yang sama yang berlaku untuk Audit Manager](#) juga berlaku dalam produk GRC pihak ketiga. Misalnya, masing-masing Akun AWS dapat memiliki hingga 100 penilaian Manajer Audit aktif. Kuota tingkat akun ini berlaku baik Anda membuat penilaian di konsol Audit Manager atau di produk GRC pihak ketiga. Sebagian besar kuota Audit Manager, tetapi tidak semua, terdaftar

di bawah AWS Audit Manager namespace di konsol Kuota Layanan. Untuk mempelajari cara meminta kenaikan kuota, lihat [Mengelola kuota Audit Manager Anda](#).

Jika Anda memiliki solusi kepatuhan dan Anda tertarik untuk mengintegrasikan dengan Manajer Audit, kirim email auditmanager-partners@amazon.com.

Third-party Produk mitra GRC yang terintegrasi dengan Audit Manager

Produk GRC pihak ketiga berikut dapat menelan bukti dari Manajer Audit.

MetricStream

Untuk menggunakan integrasi ini, hubungi [MetricStream](#) untuk akses dan pembelian perangkat lunak MetricStream GRC.

Dibangun di MetricStream atas Platform, solusi MetricStream Enterprise GRC memungkinkan pendekatan komprehensif dan kolaboratif untuk aktivitas dan proses GRC di seluruh perusahaan. Dengan memasukkan bukti dari Audit Manager ke dalam MetricStream, Anda dapat secara proaktif mengidentifikasi bukti yang tidak sesuai dari AWS lingkungan Anda dan meninjaunya bersama bukti dari sumber data lokal atau mitra cloud lainnya. Ini memberi Anda cara yang nyaman dan terpusat untuk meninjau dan meningkatkan keamanan cloud dan postur kepatuhan Anda saat Anda mempersiapkan audit.

Dengan integrasi MetricStream dan Audit Manager, Anda dapat melakukan operasi API berikut.

Tugas	Operasi API
Menyiapkan integrasi Manajer Audit	• GetAccountStatus • GetOrganizationAdminAccount • GetSettings
Meninjau sumber daya Manajer Audit	• GetAssessment • GetAssessmentFramework • GetControl • ListAssessmentFrameworks • ListControls

Tugas	Operasi API
Membuat sumber daya Audit Manager	• CreateAssessment • CreateAssessmentFramework
Memperbarui sumber daya Audit Manager	• UpdateAssessment • UpdateAssessmentControl • UpdateAssessmentStatus
Mengelola bukti	• StartQuery(AWS CloudTrail API) • GetQueryResults(AWS CloudTrail API)
Menghapus sumber daya Audit Manager	• DeleteAssessmentFramework

T MetricStream autan terkait

- [AWS Marketplace tautan](#)
- [Tautan produk](#)
- [Harga produk](#)

Mengintegrasikan bukti Audit Manager ke dalam sistem GRC Anda

Sebagai pelanggan perusahaan, Anda mungkin memiliki sumber daya di beberapa pusat data, termasuk vendor cloud lainnya dan lingkungan lokal. Untuk mengumpulkan bukti dari lingkungan ini, Anda dapat menggunakan solusi GRC (Tata Kelola, Risiko, dan Kepatuhan) pihak ketiga seperti MetricStream CyberGRC atau RSA Archer. Atau, Anda dapat menggunakan sistem GRC eksklusif yang Anda kembangkan di rumah.

Tutorial ini menunjukkan kepada Anda bagaimana Anda dapat mengintegrasikan sistem GRC internal atau eksternal Anda dengan Audit Manager. Integrasi ini memungkinkan vendor untuk mengumpulkan bukti tentang AWS penggunaan dan konfigurasi pelanggan mereka, dan mengirim bukti itu langsung dari Manajer Audit ke aplikasi GRC. Dengan melakukan ini, Anda dapat memusatkan pelaporan kepatuhan Anda di berbagai lingkungan.

Untuk tujuan tutorial ini:

1. Vendor adalah entitas atau perusahaan yang memiliki aplikasi GRC yang sedang diintegrasikan dengan Audit Manager.
2. Pelanggan adalah entitas atau perusahaan yang menggunakan AWS, dan yang juga menggunakan aplikasi GRC internal atau eksternal.

Note

Dalam beberapa kasus, aplikasi GRC dimiliki dan digunakan oleh perusahaan yang sama. Dalam skenario ini, vendor adalah grup atau tim yang memiliki aplikasi GRC, dan pelanggan adalah tim atau grup yang menggunakan aplikasi GRC.

Tutorial ini menunjukkan kepada Anda cara melakukan hal berikut:

- [Langkah 1: Aktifkan Manajer Audit](#)
- [Langkah 2: Siapkan izin](#)
- [Langkah 3. Petakan kontrol perusahaan Anda ke kontrol Audit Manager](#)
- [Langkah 4. Perbarui pemetaan kontrol Anda](#)
- [Langkah 5: Buat penilaian](#)
- [Langkah 6. Mulai mengumpulkan bukti](#)

Prasyarat

Sebelum memulai, pastikan Anda memenuhi persyaratan berikut:

- Anda memiliki infrastruktur yang berjalan di dalamnya AWS.
- Anda menggunakan sistem GRC internal, atau Anda menggunakan perangkat lunak GRC pihak ketiga yang disediakan oleh vendor.
- Anda menyelesaikan semua [prasyarat](#) yang diperlukan untuk [mengatur Audit Manager](#).
- Anda akrab dengan [Memahami AWS Audit Manager konsep dan terminologi](#).

Beberapa batasan yang perlu diingat:

- Manajer Audit adalah seorang Regional Layanan AWS. Anda harus mengatur Audit Manager secara terpisah di setiap Wilayah tempat Anda menjalankan AWS beban kerja.

- Manajer Audit tidak mendukung agregasi bukti dari beberapa Wilayah ke dalam satu Wilayah. Jika sumber daya Anda mencakup beberapa Wilayah AWS, Anda harus mengumpulkan bukti dalam sistem GRC Anda.
- Audit Manager memiliki kuota default untuk jumlah sumber daya yang dapat Anda buat. Anda dapat meminta peningkatan kuota default ini jika diperlukan. Untuk informasi selengkapnya, lihat [Kuota dan batasan untuk AWS Audit Manager](#).

Langkah 1: Aktifkan Manajer Audit

Siapa yang menyelesaikan langkah ini

Pelanggan

Apa yang perlu Anda lakukan

Mulailah dengan mengaktifkan Audit Manager untuk Anda Akun AWS. Jika akun Anda adalah bagian dari organisasi, Anda dapat mengaktifkan Audit Manager menggunakan akun manajemen Anda dan kemudian menentukan administrator yang didelegasikan untuk Manajer Audit.

Prosedur

Untuk mengaktifkan Audit Manager

Ikuti petunjuk untuk [Aktifkan Manajer Audit](#). Ulangi prosedur penyiapan untuk semua Wilayah tempat Anda ingin mengumpulkan bukti.

Tip

Jika Anda menggunakan AWS Organizations, kami sangat menyarankan Anda menyiapkan administrator yang didelegasikan selama langkah ini. Saat menggunakan akun administrator yang didelegasikan di Audit Manager, Anda dapat menggunakan pencari bukti untuk mencari bukti di semua akun anggota di organisasi Anda.

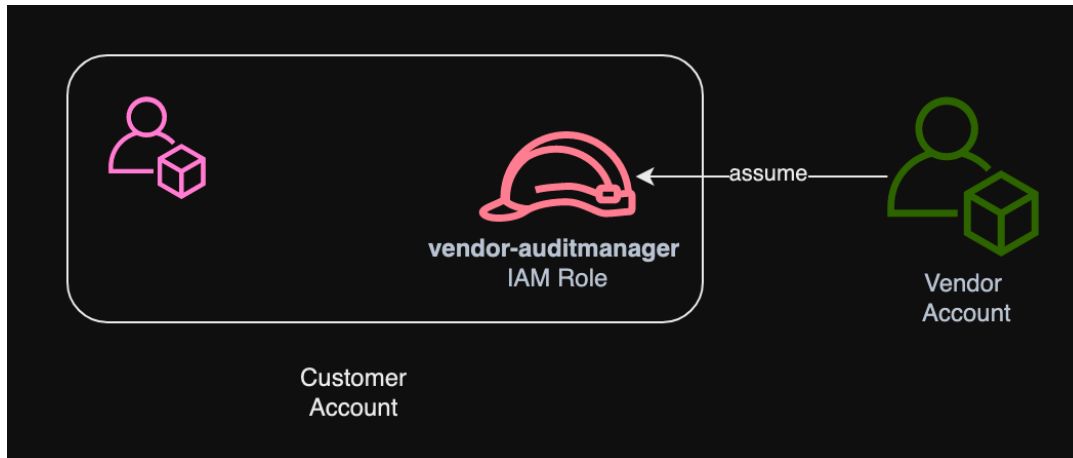
Langkah 2: Siapkan izin

Siapa yang menyelesaikan langkah ini

Pelanggan

Apa yang perlu Anda lakukan

Pada langkah ini, pelanggan membuat peran IAM untuk akun mereka. Pelanggan kemudian memberikan izin vendor untuk mengambil peran tersebut.



Prosedur

Untuk membuat peran untuk akun pelanggan

Ikuti instruksi dalam [Membuat peran untuk pengguna IAM](#) dalam Panduan Pengguna IAM.

- Pada langkah 8 alur kerja pembuatan peran, pilih **Buat kebijakan** dan masukkan kebijakan untuk peran tersebut.

Minimal, peran harus memiliki izin berikut:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AuditManagerAccess",
      "Effect": "Allow",
      "Action": [
        "auditmanager:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "OrganizationsAccess",
      "Effect": "Allow",

```

```
"Action" : [
  "organizations:ListAccountsForParent",
  "organizations:ListAccounts",
  "organizations:DescribeOrganization",
  "organizations:DescribeOrganizationalUnit",
  "organizations:DescribeAccount",
  "organizations:ListParents",
  "organizations:ListChildren"
],
"Resource" : "*"
},
{
  "Sid" : "IAMAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetUser",
    "iam:ListUsers",
    "iam:ListRoles"
  ],
  "Resource" : "*"
},
{
  "Sid" : "S3Access",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "KmsAccess",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:ListKeys",
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Sid" : "KmsCreateGrantAccess",
  "Effect" : "Allow",
  "Action" : [
    "kms:CreateGrant"
```

```

    ],
    "Resource" : "*",
    "Condition" : {
      "Bool" : {
        "kms:GrantIsForAWSResource" : "true"
      },
      "StringLike" : {
        "kms:ViaService" : "auditmanager.*.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "SNSAccess",
    "Effect" : "Allow",
    "Action" : [
      "sns:ListTopics"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "TagAccess",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : "*"
  }
]
}

```

- Pada langkah 11 alur kerja pembuatan peran, masukkan vendor-auditmanager sebagai nama Peran.

Untuk mengizinkan akun vendor untuk mengambil peran

Ikuti petunjuk dalam Mem [berikan izin pengguna untuk beralih peran](#) di Panduan Pengguna IAM.

- Pernyataan kebijakan harus mencakup Allow efek padasts:AssumeRole action.
- Itu juga harus menyertakan Nama Sumber Daya Amazon (ARN) dari peran dalam elemen Sumber Daya.
- Berikut adalah contoh pernyataan kebijakan yang dapat Anda gunakan.

Dalam kebijakan ini, ganti *placeholder text* dengan Akun AWS ID vendor Anda.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::111122223333:role/vendor-auditmanager"
  }
}
```

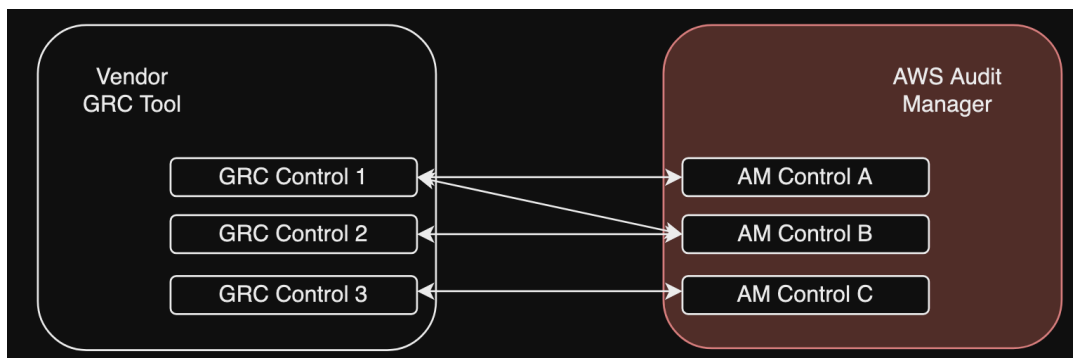
Langkah 3. Petakan kontrol perusahaan Anda ke kontrol Audit Manager

Siapa yang menyelesaikan langkah ini

Pelanggan

Apa yang perlu Anda lakukan

Vendor menyimpan daftar kontrol perusahaan yang dikuratori yang dapat digunakan pelanggan dalam penilaian. Untuk mengintegrasikan dengan Audit Manager, vendor harus membuat antarmuka yang memungkinkan pelanggan memetakan kontrol perusahaan mereka ke kontrol Manajer Audit yang sesuai. Anda dapat memetakan ke [common control](#) s (lebih disukai), atau [standard control](#) s. Anda harus menyelesaikan pemetaan ini sebelum memulai penilaian apa pun di aplikasi GRC vendor.



Opsi 1: Petakan kontrol perusahaan ke kontrol umum (disarankan)

Ini adalah cara yang disarankan untuk memetakan kontrol perusahaan Anda ke Manajer Audit. Ini karena kontrol umum sangat selaras dengan standar industri umum. Ini membuatnya lebih mudah untuk memetakannya ke kontrol perusahaan Anda.

Dengan pendekatan ini, vendor membuat antarmuka yang memungkinkan pelanggan untuk melakukan pemetaan satu kali antara kontrol perusahaan mereka dan kontrol umum yang sesuai yang disediakan oleh Audit Manager. Vendor dapat menggunakan operasi [ListControls](#), [ListCommonControls](#), dan [GetControl](#) API untuk menampilkan informasi ini kepada pelanggan. Setelah pelanggan menyelesaikan latihan pemetaan, vendor kemudian dapat menggunakan pemetaan ini untuk [membuat kontrol kustom](#) di Audit Manager.

Berikut adalah contoh pemetaan kontrol umum:

Katakanlah Anda memiliki kontrol perusahaan bernama `Asset Management`. Kontrol perusahaan ini memetakan ke dua kontrol umum di Audit Manager (`Asset performance management` dan `Asset maintenance scheduling`). Dalam hal ini, Anda harus membuat kontrol khusus di Audit Manager (kami akan menamainya `enterprise-asset-management`). Kemudian, dan tambahkan `Asset performance management` dan `Asset maintenance scheduling` sebagai sumber bukti ke kontrol kustom baru. Sumber bukti ini mengumpulkan bukti pendukung dari kelompok sumber AWS data yang telah ditentukan sebelumnya. Ini memberi Anda cara yang efisien untuk mengidentifikasi sumber AWS data yang dipetakan dengan persyaratan kontrol perusahaan Anda.

Prosedur

Untuk menemukan kontrol umum yang tersedia yang dapat Anda petakan

Ikuti langkah-langkah untuk [menemukan daftar kontrol umum yang tersedia](#) di Audit Manager.

Untuk membuat kontrol kustom

1. Ikuti langkah-langkah untuk [membuat kontrol kustom](#) yang selaras dengan kontrol perusahaan Anda.

Saat Anda menentukan sumber bukti di langkah 2 alur kerja pembuatan kontrol kustom, lakukan hal berikut:

- Pilih AWS sumber terkelola sebagai sumber bukti.
- Pilih Gunakan kontrol umum yang sesuai dengan tujuan kepatuhan Anda.

- Pilih hingga lima kontrol umum sebagai sumber bukti untuk kontrol perusahaan Anda.
2. Ulangi tugas ini untuk semua kontrol perusahaan Anda, dan buat kontrol kustom yang sesuai di Audit Manager untuk masing-masing kontrol.

Opsi 2: Petakan kontrol perusahaan ke kontrol standar

Audit Manager menyediakan sejumlah besar kontrol standar bawaan. Anda dapat melakukan pemetaan satu kali antara kontrol perusahaan Anda dan kontrol standar ini. Setelah mengidentifikasi kontrol standar yang sesuai dengan kontrol perusahaan Anda, Anda dapat menambahkan kontrol standar ini langsung ke kerangka kerja khusus. Jika Anda memilih opsi ini, Anda tidak perlu membuat kontrol kustom apa pun di Audit Manager.

Prosedur

Untuk menemukan kontrol standar yang tersedia yang dapat Anda petakan

Ikuti langkah-langkah untuk [menemukan daftar kontrol standar yang tersedia](#) di Audit Manager.

Untuk membuat kerangka kerja khusus

1. Ikuti langkah-langkah untuk [membuat kerangka kerja khusus](#) di Audit Manager.

Saat Anda menentukan kumpulan kontrol di langkah 2 prosedur pembuatan kerangka kerja, sertakan kontrol standar yang dipetakan ke kontrol perusahaan Anda.

2. Ulangi tugas ini untuk semua kontrol perusahaan Anda sampai Anda menyertakan semua kontrol standar yang sesuai dalam kerangka kustom Anda.

Langkah 4. Perbarui pemetaan kontrol Anda

Siapa yang menyelesaikan langkah ini

Vendor, pelanggan

Apa yang perlu Anda lakukan

Audit Manager terus memperbarui kontrol umum dan kontrol standar untuk memastikan bahwa mereka menggunakan sumber AWS data terbaru yang tersedia. Ini berarti bahwa kontrol pemetaan adalah tugas satu kali: Anda tidak perlu mengelola kontrol standar setelah Anda menambahkannya ke kerangka kerja khusus, dan Anda tidak perlu mengelola kontrol umum setelah Anda menambahkannya sebagai sumber bukti di kontrol kustom Anda. Setiap kali kontrol umum

diperbarui, pembaruan yang sama secara otomatis diterapkan ke semua kontrol khusus yang menggunakan kontrol umum tersebut sebagai sumber bukti.

Namun, seiring waktu, ada kemungkinan bahwa kontrol umum baru dan kontrol standar akan tersedia untuk Anda gunakan sebagai sumber bukti. Dengan pemikiran ini, vendor dan pelanggan harus membuat alur kerja untuk secara berkala mengambil kontrol umum terbaru dan kontrol standar dari Audit Manager. Anda kemudian dapat meninjau pemetaan antara kontrol perusahaan dan kontrol Audit Manager, dan memperbarui pemetaan sesuai kebutuhan.

Jika kontrol perusahaan Anda dipetakan ke kontrol umum

Selama proses pemetaan, Anda membuat kontrol khusus. Anda dapat menggunakan Audit Manager untuk mengedit kontrol kustom tersebut sehingga mereka menggunakan kontrol umum terbaru yang tersedia sebagai sumber bukti. Setelah pembaruan kontrol kustom berlaku, penilaian Anda yang ada akan secara otomatis mengumpulkan bukti terhadap kontrol kustom yang diperbarui. Tidak perlu membuat kerangka kerja atau penilaian baru.

Prosedur

Untuk menemukan kontrol umum terbaru yang dapat Anda petakan

Ikuti langkah-langkah untuk [menemukan kontrol umum yang tersedia](#) di Audit Manager.

Untuk mengedit kontrol kustom

1. Ikuti langkah-langkah untuk [mengedit kontrol kustom](#) di Audit Manager.

Saat Anda memperbarui sumber bukti di langkah 2 alur kerja pengeditan, lakukan hal berikut:

- Pilih AWS sumber terkelola sebagai sumber bukti.
 - Pilih Gunakan kontrol umum yang sesuai dengan tujuan kepatuhan Anda.
 - Pilih kontrol umum baru yang ingin Anda gunakan sebagai sumber bukti untuk kontrol kustom Anda.
2. Ulangi tugas ini untuk semua kontrol perusahaan yang ingin Anda perbarui.

Jika kontrol perusahaan Anda dipetakan ke kontrol standar

Dalam hal ini, vendor harus membuat kerangka kerja khusus baru yang mencakup kontrol standar terbaru yang tersedia, dan kemudian membuat penilaian baru menggunakan kerangka kerja baru ini. Setelah membuat penilaian baru, Anda dapat menandai penilaian lama Anda sebagai tidak aktif.

Prosedur

Untuk menemukan kontrol standar terbaru yang dapat Anda petakan

Ikuti langkah-langkah untuk [menemukan kontrol standar yang tersedia](#) di Audit Manager.

Untuk membuat kerangka kerja khusus dan menambahkan kontrol standar terbaru

Ikuti langkah-langkah untuk [membuat kerangka kerja khusus](#) di Audit Manager.

Saat Anda menentukan kumpulan kontrol di langkah 2 alur kerja pembuatan kerangka kerja, sertakan kontrol standar baru.

Untuk membuat penilaian

Buat penilaian dalam aplikasi GRC.

Untuk mengubah status penilaian menjadi tidak aktif

Ikuti langkah-langkah untuk [mengubah status penilaian](#) di Audit Manager.

Langkah 5: Buat penilaian

Siapa yang menyelesaikan langkah ini

Aplikasi GRC, dengan masukan dari vendor

Apa yang perlu Anda lakukan

Sebagai pelanggan, Anda tidak perlu membuat penilaian langsung di Audit Manager. Saat Anda memulai penilaian untuk kontrol tertentu dalam aplikasi GRC, aplikasi GRC membuat sumber daya yang sesuai untuk Anda di Audit Manager. Pertama, aplikasi GRC menggunakan pemetaan yang Anda buat untuk mengidentifikasi kontrol Audit Manager yang relevan. Selanjutnya, ia menggunakan informasi kontrol untuk membuat kerangka kerja khusus untuk Anda. Terakhir, ia menggunakan kerangka kerja khusus yang baru dibuat untuk membuat penilaian di Audit Manager.

Membuat penilaian di Audit Manager juga membutuhkan ruang [lingkup](#). Lingkup ini mengambil daftar di Akun AWS mana pelanggan ingin menjalankan penilaian dan mengumpulkan bukti. Pelanggan harus menentukan ruang lingkup ini secara langsung dalam aplikasi GRC.

Sebagai vendor, Anda perlu menyimpan `assessmentId` yang dipetakan ke penilaian yang dimulai di aplikasi GRC. Ini `assessmentId` diperlukan untuk mengambil bukti dari Manajer Audit.

Untuk menemukan ID penilaian

1. Gunakan [ListAssessments](#) operasi untuk melihat penilaian Anda di Audit Manager. Anda dapat menggunakan [parameter](#) status untuk melihat penilaian yang aktif.

```
aws auditmanager list-assessments --status ACTIVE
```

2. Dalam tanggapan, identifikasi penilaian yang ingin Anda simpan di aplikasi GRC, dan catat. `assessmentId`

Langkah 6. Mulai mengumpulkan bukti

Siapa yang menyelesaikan langkah ini

AWS Audit Manager, dengan masukan dari vendor

Apa yang perlu Anda lakukan

Setelah Anda membuat penilaian, dibutuhkan waktu hingga 24 jam untuk mulai mengumpulkan bukti. Pada titik ini, kontrol perusahaan Anda sekarang secara aktif mengumpulkan bukti untuk penilaian Manajer Audit Anda.

Kami menyarankan Anda menggunakan [fitur pencari](#) bukti untuk menanyakan dan menemukan bukti dengan cepat di Manajer Audit. Jika Anda menggunakan pencari bukti sebagai administrator yang didelegasikan, Anda dapat mencari bukti di semua akun anggota di organisasi Anda. Dengan menggunakan kombinasi filter dan pengelompokan, Anda dapat secara progresif mempersempit cakupan permintaan pencarian Anda. Misalnya, jika Anda menginginkan tampilan tingkat tinggi kesehatan sistem Anda, lakukan pencarian luas dan filter berdasarkan penilaian, rentang tanggal, dan kepatuhan sumber daya. Jika tujuan Anda adalah memperbaiki sumber daya tertentu, Anda dapat melakukan pencarian sempit untuk menargetkan bukti untuk kontrol atau ID sumber daya tertentu. Setelah menentukan filter, Anda dapat mengelompokkan dan kemudian melihat pratinjau hasil pencarian yang cocok sebelum membuat laporan penilaian.

Untuk mengaktifkan pencari bukti

- Ikuti petunjuk untuk [mengaktifkan pencari bukti](#) dari pengaturan Manajer Audit Anda.

Setelah mengaktifkan pencari bukti, Anda dapat memutuskan irama untuk mengambil bukti dari Manajer Audit untuk penilaian Anda. Anda juga dapat mengambil bukti untuk kontrol tertentu dalam

penilaian, dan menyimpan bukti dalam aplikasi GRC yang dipetakan ke kontrol perusahaan. Anda dapat menggunakan operasi API Manajer Audit berikut untuk mengambil bukti:

- [GetEvidence](#)
- [GetEvidenceByEvidenceFolder](#)
- [GetEvidenceFolder](#)
- [GetEvidenceFoldersByAssessment](#)
- [GetEvidenceFoldersByAssessmentControl](#)

Harga

Anda tidak akan dikenakan biaya tambahan untuk pengaturan integrasi ini, apakah Anda seorang vendor atau pelanggan. Pelanggan dikenakan biaya untuk bukti yang dikumpulkan di Audit Manager. Untuk informasi selengkapnya tentang harga, lihat [AWS Audit Manager Harga](#).

Sumber daya tambahan

Anda dapat mempelajari lebih lanjut tentang konsep yang diperkenalkan dalam tutorial ini dengan meninjau sumber daya berikut:

- [Penilaian](#) — Pelajari tentang konsep dan tugas untuk mengelola penilaian.
- [Pustaka kontrol](#) — Pelajari tentang konsep dan tugas untuk mengelola kontrol kustom.
- [Perpustakaan kerangka kerja](#) — Pelajari tentang konsep dan tugas untuk mengelola kerangka kerja khusus.
- [Pencari bukti](#) - Pelajari cara mengekspor file CSV atau membuat laporan penilaian dari hasil kueri Anda.
- [Pusat un](#) duhan - Pelajari cara mengunduh laporan penilaian dan ekspor CSV dari Audit Manager.

AWS Audit Manager perubahan ketersediaan

AWS Audit Manager adalah layanan yang memungkinkan Anda untuk melihat dan melaporkan postur kepatuhan AWS sumber daya Anda dengan kerangka kerja kontrol seperti SOC2, PCI DSS, dan HIPAA. Audit Manager beralih ke mode pemeliharaan dan mulai 30 April 2026 pelanggan tidak lagi dapat mengatur layanan di akun baru. Pelanggan lama yang telah menyiapkan Audit Manager untuk satu akun dalam suatu wilayah dapat terus menggunakan layanan untuk akun tersebut di wilayah tersebut, termasuk membuat Penilaian baru; tetapi mereka tidak akan dapat menyiapkan Audit Manager untuk wilayah tambahan atau akun baru. Pelanggan yang telah menyiapkan Audit Manager dalam akun manajemen organisasi akan dapat menambahkan akun dari organisasi tersebut ke penilaian; tetapi mereka tidak akan dapat memperluas penggunaan ke wilayah tambahan atau mengatur Audit Manager untuk organisasi baru.

Saat dalam mode pemeliharaan, tim layanan akan terus mendukung layanan. Ini termasuk perbaikan kode dan memelihara pemetaan sumber data untuk kerangka kerja yang saat ini didukung. Namun, tim layanan tidak akan membangun fitur baru, atau menambahkan dukungan untuk kerangka kerja baru atau versi baru dari kerangka kerja yang ada, atau menambahkan dukungan wilayah baru.

Pelanggan yang mencari solusi manajemen kepatuhan didorong untuk mengeksplorasi Paket Kesesuaian di. AWS Config Conformance Packs menyediakan sarana untuk menyebarkan dan memantau kontrol detektif, dalam bentuk Aturan Config, di beberapa akun dan wilayah. Mereka menawarkan [template pra-bangun untuk kerangka kerja umum](#) (seperti HIPAA, NIST, PCI-DSS) dan memungkinkan pembuatan aturan khusus. Paket Kesesuaian dapat dikelola pada tingkat satu akun atau di [semua akun anggota dalam organisasi di](#). AWS Organizations

Setelah menerapkan Paket Kesesuaian, Anda dapat melihat status kepatuhan sumber daya Anda dalam dasbor terkait. Atau, Anda dapat menggunakan [Dasbor Kepatuhan Sumber Daya Config](#) untuk melihat inventaris AWS sumber daya Anda, beserta status kepatuhannya, di beberapa AWS akun dan Wilayah.

Batasan Paket Kesesuaian untuk pelanggan Audit Manager

AWS Config saat ini tidak menawarkan template Conformance Pack untuk semua kerangka kerja yang didukung oleh Audit Manager, termasuk dan GDPR. SOC2 Tabel di bawah ini menyediakan pemetaan, menyoroti di mana kesenjangan ada saat ini. [Untuk pembaruan pada template Conformance Pack yang tersedia, rujuk dokumentasi produk.](#)

AWS Config tidak menyediakan fitur pelaporan audit yang secara langsung setara dengan ekspor Audit Manager. Namun, pelanggan dapat mengekspor bukti untuk mendukung Status Kepatuhan dari AWS Config menggunakan satu atau beberapa mekanisme yang dijelaskan di bagian di bawah ini.

Dari dasbor Paket Kesesuaian, pelanggan dapat melihat status kepatuhan untuk setiap Aturan Konfigurasi terkait. Pelanggan dapat menelusuri aturan dan melihat status masing-masing sumber daya individu dan bukti, dalam bentuk Item Konfigurasi untuk sumber daya tersebut.

AWS Config hanya mencatat Item Konfigurasi (CIs) sebagai bukti kepatuhan. Tidak seperti Audit Manager, Audit Manager tidak mengumpulkan AWS CloudTrail log, AWS Security Hub Kontrol, atau melakukan panggilan API ke layanan target. Bukti yang dikumpulkan AWS Config kurang lengkap, tetapi lebih mudah dinavigasi. Semua bukti yang dikumpulkan oleh AWS Config dipetakan ke status kepatuhan untuk AWS sumber daya, melalui Aturan Config. Akibatnya, tidak seperti Audit Manager, AWS Config tidak menyajikan bukti 'tidak konklusif'.

AWS Audit Manager Kerangka Pemetaan ke AWS Config Paket Kesesuaian

AWS Audit Manager Kerangka	AWS Config Templat Paket Kesesuaian
ACSC Essential Delapan	Praktik Terbaik Operasional untuk ACSC Essential 8
ACSC ISM 02 Maret 2023	Praktik Terbaik Operasional untuk ACSC ISM - Bagian 1; Praktik Terbaik Operasional untuk ACSC ISM - Bagian 2
Kerangka Contoh Audit Manager	- Tidak ada yang setara -
AWS Control Tower Pagar pembatas	AWS Control Tower Paket Kesesuaian Detective Guardrails
AWS Kerangka Praktik Terbaik AI Generatif v2	Praktik Terbaik Operasional untuk AI dan ML
AWS License Manager	- Tidak ada yang setara -
AWS Praktik Terbaik Keamanan Dasar	Praktik Terbaik Operasional untuk AWS Pilar Keamanan Kerangka Kerja yang Dirancang

AWS Audit Manager Kerangka	AWS Config Templat Paket Kesesuaian
	dengan Baik, ditambah paket Praktik Terbaik Keamanan untuk beberapa layanan individual
AWS Praktik Terbaik Operasional	- Tidak ada yang setara -
AWS Kerangka Kerja Well-Architected WAF v10	Praktik Terbaik Operasional untuk Pilar Keandalan Kerangka AWS Kerja yang Dirancang dengan Baik; Praktik Terbaik Operasional untuk Pilar Keamanan Kerangka Kerja yang Dirancang AWS dengan Baik
Kontrol Awan Menengah CCCS	Praktik Operasional-Terbaik-untuk-CCCS-Medium
Tolok Ukur CIS v1.2.0 AWS	- Tidak ada yang setara -
Tolok Ukur CIS v1.3.0 AWS	- Tidak ada yang setara -
Tolok Ukur CIS v1.4.0 AWS	Praktik Operasional-Terbaik-untuk-CIS-AWS-v1.4-Level1; -CIS-AWS-v1.4-Level2 Operational-Best-Practices-for
Kontrol CIS v7.1, IG1	- Tidak ada yang setara -
Kontrol Keamanan Kritis CIS versi 8.0, IG1	Praktik terbaik-operasional-untuk-CIS-kritis-keamanan-kontrol-v8- IG1
Kontrol Dasar Keamanan FedRAMP r4	Praktik Operasional-Terbaik-untuk-FedRAMP (Rendah); -FedRAMP (Sedang); Operational-Best-Practices-for -FedRAMP (Bagian Tinggi 1); -FedRAMP (Bagian Tinggi 2 Operational-Best-Practices-for) Operational-Best-Practices-for
GDPR 2016	- Tidak ada yang setara -
Gramm-Leach-Bliley Bertindak	Praktik Operasional-Terbaik-untuk-Gramm-Leach-Bliley-Act

AWS Audit Manager Kerangka	AWS Config Templat Paket Kesesuaian
Judul 21 CFR Bagian 11	Praktik Operasional-Terbaik-untuk-FDA-21CFR-Bagian-11
Lampiran GMP UE 11, v1	Praktik Operasional-Terbaik-untuk-GXP-EU-Annex-11
Aturan Keamanan HIPAA: Feb 2003	Praktik Operasional-Terbaik-untuk-HIPAA-Security
Aturan Akhir Omnibus HIPAA	Praktik Operasional-Terbaik-untuk-HIPAA-Security
ISO/IEC 27001:2013 Lampiran A	- Tidak ada yang setara -
NIST SP 800-53 Rev 5	Praktik Operasional-Terbaik-untuk-NIST-800-53-REV-5
Kerangka Keamanan Siber NIST v1.1	Praktik Operasional-Terbaik-untuk-NIST-CSF
NIST SP 800-171 Rev 2	Praktik Operasional-Terbaik-Untuk-NIST-800-171
PCI DSS V3.2.1	Praktik Terbaik Operasional untuk PCI DSS 3.2.1
PCI DSS V4.0	Praktik Operasional-Terbaik-untuk-PCI-DSS-V4.0
SSAE-18 SOC 2	- Tidak ada yang setara -

Mengekspor bukti dari AWS Config

AWS Config Kueri Lanjutan (Direkomendasikan untuk mengekspor Item Konfigurasi sumber daya individu sebagai bukti)

Anda dapat menggunakan kueri SQL di AWS Config konsol untuk memilih sumber daya tertentu dan mengekspor konfigurasinya saat ini dalam format CSV atau JSON.

- Bagaimana: Pergi AWS Config ke> Kueri lanjutan.
- Contoh Kueri:

```
SELECT resourceId, resourceType, configuration, tags, compliance
WHERE resourceType = 'AWS::EC2::Instance'
AND resourceId = 'i-xxxxxxxxx'
```

- Ekspor: Pilih “Jalankan” dan kemudian “Ekspor hasil” ke CSV.
- Terbaik untuk: Laporan yang dikurasi pada subset sumber daya.

GetResourceConfigHistory API (Direkomendasikan untuk riwayat lengkap)

Jika auditor perlu melihat status kepatuhan sumber daya selama periode waktu tertentu (bukan hanya status saat ini), gunakan CLI/API.

- Caranya: Gunakan `get-resource-config-history` perintah di AWS CLI.
- Contoh Perintah:

```
aws configservice get-resource-config-history \
  --resource-type AWS::EC2::Instance \
  --resource-id i-xxxxxxxxx \
  --region us-east-1
```

- Output: Mengembalikan objek JSON terperinci dari perubahan konfigurasi, termasuk status kepatuhan pada saat setiap perubahan.

Amazon Athena dan Amazon Quick (Direkomendasikan untuk kueri yang difilter di berbagai sumber daya)

Pelanggan dapat menggunakan Amazon Athena untuk membuat dan menjalankan kueri berbasis SQL terhadap data konfigurasi sumber daya yang direkam oleh AWS Config. Pelanggan juga dapat mengimpor data ke Amazon Quick untuk membuat analisis dan dasbor. Untuk informasi selengkapnya, lihat [Memvisualisasikan AWS Config data menggunakan Amazon Athena dan Amazon Quick](#).

Membandingkan solusi kepatuhan

Fitur	AWS Audit Manager	AWS Config — Paket Kesesuaian
Kontrol Terkelola	Menyediakan 35 kerangka kerja terkelola, termasuk kerangka peraturan dan industri, seperti, PCI DSS SOC2, dan HIPAA, dan kerangka kerja praktik terbaik. AWS	Menyediakan lebih dari 100 templat Paket Kesesuaian yang telah ditentukan sebelumnya - termasuk paket peraturan dan industri, seperti PCI DSS, dan HIPAA, dan paket praktik Terbaik Operasional. AWS
Kustomisasi	Buat Kontrol kustom dan Kerangka kustom.	Buat Aturan kustom dan templat yang ditentukan sendiri .
Penyiapan	Buat Penilaian berdasarkan kerangka kerja.	Menyebarkan Paket Kesesuaian.
Pengumpulan bukti	Mengumpulkan bukti dari empat sumber data: (1) Panggilan API Layanan, (2) AWS Security Hub kontrol, (3) AWS CloudTrail peristiwa, (4) Aturan Konfigurasi. Pelanggan harus terlebih dahulu menerapkan Aturan menggunakan AWS Config atau AWS Control Tower.	Merekam bukti sebagai Item Konfigurasi yang mendukung evaluasi Aturan Config.
Dasbor kepatuhan	Dasbor penilaian memberikan snapshot harian dan tampilan kontrol dengan bukti yang tidak sesuai.	Dasbor Conformance Pack memberikan skor kepatuhan keseluruhan, garis waktu kepatuhan, dan tampilan berdasarkan

Fitur	AWS Audit Manager	AWS Config — Paket Kesesuaian
		Aturan. Telusuri untuk melihat postur kepatuhan berdasarkan sumber daya dan bukti pendukung, dalam bentuk Item Konfigurasi.
Remediasi sumber daya yang tidak sesuai	Tidak didukung.	Pelanggan dapat menentukan dan memulai rencana remediasi.
Format bukti	Hasil evaluasi Aturan Konfigurasi; Hasil panggilan API individual, misalnya iam.getPolicy; temuan. AWS Security Hub	Hasil evaluasi Aturan Konfigurasi; Item Konfigurasi.
Pelaporan Audit	Bukti dapat dipilih untuk dimasukkan dalam Laporan Audit, yang dapat diekspor dalam format PDF. Juga, mendukung ekspor format CSV dari alat pencari bukti.	Item Konfigurasi Individu dapat diekspor melalui alat Config Advance Query. Pelanggan dapat membuat skrip CLI untuk mengekspor bukti melalui layanan. APIs

Menonaktifkan AWS Audit Manager

Menonaktifkan Audit Manager menghentikan pengumpulan bukti baru, tetapi tidak menghapus bukti yang ada, kecuali Anda secara eksplisit memilih opsi ini. Bukti akan disimpan selama dua tahun sejak tanggal pengumpulannya. Sebagai pelanggan yang sudah ada, Anda dapat mengaktifkan kembali layanan untuk mendapatkan akses ke bukti dan memulai kembali pengumpulan bukti.

Pelanggan dapat menonaktifkan Audit Manager untuk akun, baik melalui tab pengaturan di konsol atau CLI.

Pelanggan yang telah menggunakan Audit Manager untuk Organisasi harus menonaktifkan layanan dari Akun Manajemen Organisasi. Secara default, akun administrator yang didelegasikan tidak memiliki izin yang diperlukan untuk menonaktifkan Audit Manager untuk Organisasi.

Sumber daya tambahan

- AWS Config — Dokumentasi Paket [Kesesuaian](#)
- AWS Audit Manager — [Dokumentasi Penemu Bukti](#)

Pertanyaan yang Sering Diajukan

Apakah AWS Audit Manager layanan sedang dimatikan?

Tidak. Layanan Audit Manager sedang dipindahkan ke mode pemeliharaan. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa.

Mengapa AWS memindahkan Audit Manager ke mode pemeliharaan?

Kami dapat memberikan pengalaman pelanggan yang lebih baik dan lebih terintegrasi dengan berinvestasi AWS Config untuk Manajemen Kepatuhan.

Dapatkah saya menggunakan AWS Config untuk Manajemen Kepatuhan hari ini?

Ya. Conformance Packs in AWS Config dapat digunakan sebagai alat untuk mengelola kepatuhan AWS sumber daya dengan kerangka kerja seperti PCI DSS, FedRAMP, dan HIPAA. Conformance Packs memungkinkan pelanggan untuk secara kolektif menyebarkan kontrol detektif untuk kerangka kerja yang berbeda dan menyediakan dasbor yang menunjukkan kepatuhan tingkat sumber daya.

Apa manfaat migrasi untuk digunakan AWS Config untuk Manajemen Kepatuhan?

Bagi pelanggan yang mencari solusi untuk memantau kepatuhan AWS sumber daya dengan kerangka kerja seperti PCI DSS, Paket Kesesuaian dalam AWS Config menyediakan solusi yang lebih lengkap dan dapat ditindaklanjuti. Pelanggan dapat (1) menerapkan kontrol detektif untuk akun individu atau seluruh organisasi, (2) mengakses dasbor yang menampilkan skor kepatuhan, (3) menelusuri dan melihat status kepatuhan sumber daya individu, (4) mengakses garis waktu untuk sumber daya yang menunjukkan bagaimana postur kepatuhan berubah dari waktu ke waktu, (4) menarik bukti, dalam bentuk Item Konfigurasi, yang mendukung status kepatuhan sumber daya untuk kontrol.

Apakah Paket Kesesuaian merupakan pengganti langsung untuk kerangka kerja di AWS Config Audit Manager?

Tidak. Paket Kesesuaian adalah alat yang ampuh yang dapat digunakan pelanggan untuk mengelola postur kepatuhan sumber daya mereka. AWS Namun, Paket Kesesuaian tidak setara dengan Audit Manager Frameworks. Template Conformance Pack yang disediakan untuk kerangka kerja seperti PCI DSS hanya berisi Kontrol Inti teknis yang dapat dievaluasi sebagai Aturan Config. Template Conformance Pack tidak berisi set lengkap kontrol audit yang harus dipenuhi organisasi untuk lulus Audit PCI DSS; tidak ada Aturan Config yang memverifikasi bahwa organisasi telah mendokumentasikan Kebijakan Keamanan dan prosedur Operasionalnya. Meskipun dasbor Compliance Pack memberikan sinyal yang jelas tentang postur kepatuhan AWS sumber daya Anda yang dievaluasi oleh Aturan Konfigurasi, AWS Config tidak menawarkan solusi manajemen kepatuhan umum untuk menangkap, mengatur, dan berbagi bukti untuk rangkaian lengkap kontrol yang diperlukan oleh kerangka kerja seperti PCI DSS. Pelanggan yang mencari solusi untuk masalah ini didorong untuk mempertimbangkan solusi mitra, seperti yang dari Vanta dan Drata, yang dapat digunakan bersama dengan AWS Config untuk memberikan solusi otomatisasi end-to-end kepatuhan.

Apakah ada Paket Kesesuaian untuk semua kerangka kerja yang didukung oleh Audit Manager?

Tidak, saat ini ada sejumlah kerangka kerja di Audit Manager yang tidak memiliki Paket Kesesuaian yang sesuai. AWS Config Tabel di atas menyediakan pemetaan dari framework Audit Manager ke Config Conformance Packs. Kesenjangan yang paling menonjol adalah SOC2 dan GDPR. Harap pantau pengumuman AWS Config 'Apa yang Baru' untuk pembaruan tentang rilis Conformance Pack yang baru. Selain template Paket Kesesuaian yang telah ditentukan sebelumnya yang disediakan oleh AWS, pelanggan dapat menentukan templat Paket Kesesuaian mereka sendiri yang mengelompokkan bersama dengan Aturan Konfigurasi dan memungkinkan pelanggan menentukan tindakan remediasi untuk sumber daya yang tidak sesuai.

Dapatkah pelanggan mengeksport bukti untuk auditor menggunakan? AWS Config

AWS Config menyediakan beberapa alat untuk mengeksport bukti kepatuhan sumber daya. Lihat [Halaman Perubahan Ketersediaan](#) untuk panduan tentang penggunaan alat ini.

Sebagai pelanggan yang sudah ada, dapatkah saya terus menggunakan Audit Manager seperti biasa?

Ya. Sebagai pelanggan lama, Anda dapat terus menggunakan Audit Manager seperti biasa, termasuk membuat dan memelihara Penilaian, meninjau bukti, dan menghasilkan Laporan Audit. Pelanggan yang telah menggunakan Audit Manager di seluruh organisasi mereka dapat memperluas Penilaian untuk menyertakan Akun baru dari Organisasi.

Sebagai pelanggan lama dengan penerapan satu akun, dapatkah saya menerapkan Audit Manager untuk Organisasi saya?

Tidak. Mulai 30 April 2026, pelanggan dengan penerapan akun tunggal tidak akan dapat menerapkan Audit Manager di seluruh Organisasi.

Bagaimana cara memeriksa apakah Audit Manager diatur dalam akun?

Untuk penerapan akun tunggal, pelanggan dapat masuk ke akun dan menavigasi di dalam konsol ke layanan Audit Manager untuk melihat apakah Audit Manager disiapkan dalam akun tersebut. Untuk Organizations, pelanggan harus melakukan ini dari dalam Akun Manajemen.

Bagaimana cara menonaktifkan Audit Manager?

Pelanggan dapat menonaktifkan Audit Manager untuk akun, baik melalui tab pengaturan di konsol atau CLI. Pelanggan yang telah menggunakan Audit Manager untuk Organisasi harus menonaktifkan layanan dari Akun manajemen Organisasi; secara default akun Administrator yang didelegasikan untuk Audit Manager tidak memiliki izin yang diperlukan. Menonaktifkan Audit Manager menghentikan pengumpulan bukti baru, tetapi tidak menghapus bukti yang ada, kecuali Anda secara eksplisit memilih opsi ini. Bukti akan disimpan selama dua tahun sejak tanggal pengumpulannya. Sebagai pelanggan yang sudah ada, Anda dapat mengaktifkan kembali layanan untuk mendapatkan akses ke bukti dan memulai kembali pengumpulan bukti.

Bagaimana saya bisa terus mengakses bukti setelah saya menonaktifkan Audit Manager?

Cara termudah untuk terus mengakses bukti yang dikumpulkan oleh Audit Manager adalah dengan mengaktifkan Evidence Finder terlebih dahulu, sebelum menonaktifkan layanan. Ketika Anda mengaktifkan Audit Manager Evidence Finder mengeksport bukti ke CloudTrail data lake, yang akan dapat terus Anda akses setelah Anda menonaktifkan Audit Manager.

Bagaimana saya bisa menggunakan AWS Control Tower manajemen kepatuhan?

AWS Control Tower menyediakan katalog kontrol preventif, proaktif, dan detektif (diimplementasikan sebagai Aturan Config) yang dikunci oleh kerangka kerja. Ini memungkinkan Anda untuk menerapkan semua kontrol yang relevan dengan [kerangka kerja ini](#) ke satu atau lebih OUs dalam organisasi Anda. Dengan pengalaman kontrol baru saja, bukan lagi prasyarat bahwa organisasi dibuat sebagai Zona Pendaratan. Manfaatnya AWS Control Tower adalah memberi Anda pandangan tingkat U tentang sumber daya yang tidak sesuai. AWS Control Tower tidak menggunakan Paket Kesesuaian untuk menerapkan Aturan Konfigurasi dan oleh karena itu Anda tidak akan melihat Paket Kesesuaian kecuali Anda juga menerapkan Paket Kesesuaian. Juga tidak mendukung alur kerja remediasi.

Bagaimana saya bisa menggunakan AWS Security Hub CSPM manajemen kepatuhan?

Untuk kerangka kerja yang dipetakan ke standar keamanan, AWS Security Hub CSPM berikan alternatif AWS Config untuk Manajemen Kepatuhan dan remediasi dalam satu akun. Mengaktifkan standar dari dalam konsol CSPM Security Hub menerapkan serangkaian aturan terkait layanan untuk kerangka kerja terkait. Pelanggan dapat melihat dasbor kepatuhan yang menunjukkan skor kepatuhan keseluruhan dan status untuk setiap kontrol, dengan opsi untuk menelusuri ke tingkat sumber daya individu. Security Hub CSPM memungkinkan pelanggan untuk mengunduh temuan untuk aturan dalam format json dan menambahkan peringkat keparahan untuk kontrol yang membantu pelanggan memprioritaskan rencana remediasi. Dengan konfigurasi pusat, Anda dapat mengonfigurasi CSPM Security Hub di beberapa Wilayah, akun, dan unit organisasi (OU). Namun, Security Hub CSPM [menyediakan standar keamanan](#) hanya untuk sejumlah kerangka kerja terbatas, termasuk NIST 800-53 dan PCI-DSS.

Kerangka kerja yang didukung di AWS Audit Manager

Saat menjelajahi pustaka kerangka kerja di AWS Audit Manager, Anda akan menemukan daftar lengkap kerangka kerja standar pra-bangun yang dapat membantu Anda merampingkan upaya kepatuhan Anda. Kerangka kerja prebuilt ini didasarkan pada praktik AWS terbaik untuk berbagai standar dan peraturan kepatuhan. Anda dapat menggunakan kerangka kerja ini untuk membantu Anda dengan persiapan audit Anda, apakah Anda perlu menilai lingkungan Anda terhadap HIPAA, PCI DSS, SOC 2, atau lebih.

Note

Jika Anda baru mengenal Audit Manager, mulailah dengan AWS Audit Manager Sample Framework. Kerangka kerja ini dirancang untuk tujuan pembelajaran dan tidak mendukung standar kepatuhan tertentu. Ini menyediakan lingkungan yang terkendali bagi Anda untuk menjelajahi fungsionalitas inti Manajer Audit dalam lingkup yang dapat dikelola. Setelah Anda menggunakan kerangka kerja sampel untuk membiasakan diri dengan Audit Manager, Anda akan siap menggunakan kerangka kerja lain untuk penilaian kepatuhan aktual.

Daftar berikut memberikan ikhtisar kerangka kerja yang tersedia sehingga Anda dapat dengan mudah mengidentifikasi kerangka kerja yang sesuai dengan kebutuhan spesifik Anda. Luangkan waktu sejenak untuk meninjau daftar dan biasakan diri Anda dengan kerangka kerja yang paling relevan dengan kebutuhan organisasi Anda. Buka halaman mana pun untuk melihat ikhtisar kerangka kerja tersebut dan pelajari bagaimana Anda dapat menggunakannya untuk membuat penilaian dan mulai mengumpulkan bukti di Audit Manager.

Topik

- [ACSC Essential Delapan](#)
- [ACSC ISM 02 Maret 2023](#)
- [AWS Audit Manager Contoh Kerangka](#)
- [AWS Control Tower Pagar pembatas](#)
- [AWS Kerangka Praktik Terbaik AI Generatif v2](#)
- [AWS License Manager](#)
- [AWS Praktik Terbaik Keamanan Dasar](#)

- [AWS Praktik Terbaik Operasional](#)
- [AWS Kerangka Kerja yang Diarsiteksikan dengan Baik WAF v10](#)
- [Kontrol Awan Menengah CCCS](#)
- [AWS Tolok Ukur CIS v1.2.0](#)
- [AWS Tolok Ukur CIS v1.3.0](#)
- [AWS Tolok Ukur CIS v1.4.0](#)
- [Kontrol CIS v7.1, IG1](#)
- [Kontrol Keamanan Kritis CIS versi 8.0, IG1](#)
- [Kontrol Dasar Keamanan FedRAMP r4](#)
- [GDPR 2016](#)
- [Gramm-Leach-Bliley Bertindak](#)
- [Judul 21 CFR Bagian 11](#)
- [Lampiran GMP UE 11, v1](#)
- [Aturan Keamanan HIPAA: Feb 2003](#)
- [Aturan Akhir Omnibus HIPAA](#)
- [ISO/IEC 27001:2013 Lampiran A](#)
- [NIST SP 800-53 Rev 5](#)
- [Kerangka Keamanan Siber NIST v1.1](#)
- [NIST SP 800-171 Rev 2](#)
- [PCI DSS V3.2.1](#)
- [PCI DSS V4.0](#)
- [SSAE-18 SOC 2](#)

ACSC Essential Delapan

AWS Audit Manager menyediakan kerangka kerja standar bawaan yang mendukung Australian Cyber Security Center (ACSC) Essential Eight.

Topik

- [Apa itu Essential Eight ACSC?](#)

- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu Essential Eight ACSC?

ACSC adalah lembaga utama pemerintah Australia untuk keamanan siber. Untuk melindungi dari ancaman cyber, ACSC merekomendasikan agar organisasi menerapkan delapan strategi mitigasi penting dari Strategi ACSC untuk Memitigasi Insiden Keamanan Siber sebagai dasar. Garis dasar ini, yang dikenal sebagai Essential Eight, membuat musuh lebih sulit untuk mengkompromikan sistem.

Karena Essential Eight menguraikan serangkaian tindakan pencegahan minimum, organisasi Anda perlu menerapkan langkah-langkah tambahan yang dijamin oleh lingkungan Anda. Lebih lanjut, sementara Essential Eight dapat membantu mengurangi sebagian besar ancaman cyber, itu tidak akan mengurangi semua ancaman cyber. Dengan demikian, strategi mitigasi tambahan dan kontrol keamanan perlu dipertimbangkan, termasuk yang dari Strategi untuk Memitigasi Insiden Keamanan Siber dan Manual Keamanan Informasi (ISM).

The [Essential Eight](#) oleh [ACSC](#) dilisensikan di bawah [Lisensi Internasional Creative Commons Attribution 4.0](#) dan informasi hak cipta dapat ditemukan di [ACSC](#) | Hak Cipta. © Persemakmuran Australia 2022.

Menggunakan Framework ini

Anda dapat menggunakan kerangka kerja standar Essential Eight AWS Audit Manager untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan Essential Eight. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka Esential Eight. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil

penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Pusat Keamanan Cyber Australia (ACSC) Delapan Penting	61	132	3

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM. Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file -Essential-Eight.zip [AuditManager_ ConfigDataSourceMappings _Australian-Cyber-Security-Center](#) - (ACSC).

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan kontrol Essential Eight. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit ACSC. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [ACSC Essential Delapan](#)

ACSC ISM 02 Maret 2023

AWS Audit Manager menyediakan kerangka kerja standar bawaan yang mendukung Australian Cyber Security Center (ACSC) Information Security Center (ACSC) Information Security Manual (ISM).

Topik

- [Apa itu ACSC ISM?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu ACSC ISM?

ACSC adalah lembaga utama pemerintah Australia untuk keamanan siber. ACSC menghasilkan ISM, yang berfungsi sebagai seperangkat prinsip keamanan cyber. Tujuan dari prinsip-prinsip ini adalah untuk memberikan panduan strategis tentang bagaimana organisasi dapat melindungi sistem dan data mereka dari ancaman cyber. Prinsip-prinsip keamanan cyber ini dikelompokkan menjadi empat kegiatan utama: mengatur, melindungi, mendeteksi, dan merespons. Sebuah organisasi harus dapat menunjukkan bahwa prinsip-prinsip keamanan cyber sedang dipatuhi dalam organisasi mereka. ISM ditujukan untuk Chief Information Security Officers, Chief Information Officer, profesional keamanan cyber, dan manajer teknologi informasi.

Kerangka kerja ISM disediakan oleh ACSC di bawah [Lisensi Internasional Creative Commons Attribution 4.0](#), dan informasi hak cipta dapat ditemukan di [ACSC](#) | Hak Cipta. © Persemakmuran Australia 2022.

Menggunakan Framework ini

Anda dapat menggunakan kerangka kerja standar ACSC ISM AWS Audit Manager untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan

deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan ACSC ISM. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka ACSC ISM. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Panduan Keamanan Informasi (ISM) Pusat Keamanan Cyber Australia (ACSC) 02 Maret 2023	88	789	22

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM. Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file [AuditManager_ConfigDataSourceMappings_Australian-Cyber-Security-Center-\(ACSC\)-Information-Security-Manual-\(ISM\)-02-March-2023.zip](#).

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan kontrol Manual Keamanan Informasi ACSC. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit ACSC. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [Manual Keamanan Informasi ACSC](#)

AWS Audit Manager Contoh Kerangka

Jika Anda baru mengenal Audit Manager, Anda dapat menggunakan AWS Audit Manager Sample Framework untuk mengetahui cara kerja Audit Manager. Ini menyediakan lingkungan sederhana di mana Anda dapat menjelajahi fungsionalitas Audit Manager tanpa kewalahan oleh bukti yang berlebihan atau melebihi batas Anda AWS Tingkat Gratis . Setelah Anda mencoba kerangka kerja sampel, Anda akan siap untuk mulai menggunakan sisa kerangka kerja yang disediakan Audit Manager.

Topik

- [Apa itu Kerangka AWS Audit Manager Sampel?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)

Apa itu Kerangka AWS Audit Manager Sampel?

Kerangka kerja sampel menyediakan cara yang efisien dan ramah pemula untuk mengeksplorasi fungsionalitas inti Audit Manager - mengumpulkan bukti dan melampirkannya ke kontrol.

Dalam kerangka kerja, Anda akan menemukan contoh kontrol yang menunjukkan berbagai sumber data yang digunakan Audit Manager untuk mengumpulkan bukti secara otomatis. Sumber data ini mencakup AWS CloudTrail peristiwa, AWS Config aturan, AWS Security Hub CSPM kontrol, dan panggilan AWS API. Dengan menggunakan sumber data ini dalam penilaian pengujian, Anda dapat melihat cara kerja Audit Manager dengan cara yang berbeda Layanan AWS untuk mengumpulkan bukti. Selain mendemonstrasikan pengumpulan bukti otomatis, kerangka kerja sampel menunjukkan bagaimana Anda dapat menambahkan bukti Anda sendiri secara manual. Ini juga memiliki kontrol manual yang memungkinkan Anda mengunggah file sebagai bukti. Dengan mencoba kontrol otomatis dan manual, Anda dapat mengembangkan pemahaman menyeluruh tentang berbagai cara di mana bukti dapat ditambahkan ke penilaian Anda.

Note

Kerangka kerja ini berbeda dari kerangka kerja standar lainnya. Kerangka kerja sampel tidak dimaksudkan untuk mengelola penilaian atau audit kepatuhan aktual. Tujuannya adalah untuk membantu Anda mempelajari cara menggunakan Audit Manager. Ini menyediakan lingkungan yang terkendali di mana Anda dapat mengumpulkan cukup bukti untuk mengalami kemampuan Manajer Audit, sambil menjaga ruang lingkup yang dapat dikelola untuk pemula.

Menggunakan Framework ini

Menggunakan Kerangka Kerja AWS Audit Manager Sampel memungkinkan Anda berlatih menavigasi antarmuka Audit Manager, mengumpulkan bukti, dan melihat bagaimana bukti tersebut dilampirkan pada kontrol penilaian Anda.

Untuk memulai, gunakan kerangka kerja sampel untuk membuat penilaian. Tindakan ini memulai pengumpulan bukti yang sedang berlangsung untuk masing-masing kontrol otomatis dalam kerangka sampel. Berdasarkan definisi kontrol, Audit Manager menilai AWS sumber daya Anda, mengumpulkan bukti yang relevan, dan kemudian melampirkannya ke kontrol dalam penilaian Anda. Pada saat ini, Anda dapat menjelajahi bukti yang telah dikumpulkan oleh Audit Manager. Anda juga dapat mencoba menambahkan bukti Anda sendiri ke kontrol manual.

Anda dapat menemukan kerangka kerja ini di bawah tab Kerangka standar pada pustaka kerangka kerja di Audit Manager.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Amazon Web Services (AWS) Contoh Kerangka Kerja Audit Manager	4	1	2

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM. Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file [AuditManager_ConfigDataSourceMappings_AWS-Audit-Manager-Sample-Framework.zip](#).

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

AWS Control Tower Pagar pembatas

AWS Audit Manager menyediakan kerangka kerja AWS Control Tower Guardrails bawaan untuk membantu Anda dengan persiapan audit Anda.

Topik

- [Apa itu AWS Control Tower?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu AWS Control Tower?

AWS Control Tower adalah layanan manajemen dan tata kelola yang dapat Anda gunakan untuk menavigasi melalui proses pengaturan dan persyaratan tata kelola yang terlibat dalam menciptakan lingkungan AWS multi-akun.

Dengan AWS Control Tower, Anda dapat menyediakan baru Akun AWS yang sesuai dengan kebijakan perusahaan atau organisasi Anda dalam beberapa klik. AWS Control Tower membuat lapisan orkestrasi atas nama Anda yang menggabungkan dan mengintegrasikan kemampuan beberapa lainnya. [Layanan AWS](#) Layanan ini termasuk AWS Organizations, AWS IAM Identity Center, dan Layanan AWS Katalog. Ini membantu merampingkan proses pengaturan dan pengaturan AWS lingkungan multi-akun yang aman dan sesuai.

Kerangka AWS Control Tower Guardrails berisi semua Aturan AWS Config yang didasarkan pada pagar pembatas dari. AWS Control Tower

Menggunakan Framework ini

Anda dapat menggunakan kerangka kerja AWS Control Tower Guardrails untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan menurut Aturan AWS Config yang didasarkan pada pagar pembatas dari. AWS Control Tower Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk AWS Control Tower audit. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka AWS Control Tower Guardrails. Saat tiba

waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja AWS Control Tower Guardrails adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
AWS Control Tower Pagar pembatas	14	0	5

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file [AuditManager_ ConfigDataSourceMappings _AWS-Control-Tower-Guardrails.zip](#).

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan AWS Control Tower Guardrails. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [AWS Control Tower halaman layanan](#)
- [AWS Control Tower panduan pengguna](#)

AWS Kerangka Praktik Terbaik AI Generatif v2

Note

Pada 11 Juni 2024, AWS Audit Manager meningkatkan kerangka kerja ini ke versi baru, kerangka praktik terbaik AI AWS generatif v2. Selain mendukung praktik terbaik untuk Amazon Bedrock, v2 memungkinkan Anda mengumpulkan bukti yang menunjukkan bahwa Anda mengikuti praktik terbaik di Amazon SageMaker AI.

Kerangka praktik terbaik AI AWS generatif v1 tidak lagi didukung. Jika sebelumnya Anda membuat penilaian dari kerangka kerja v1, penilaian Anda yang ada akan terus berfungsi. Namun, Anda tidak dapat lagi membuat penilaian baru dari kerangka kerja v1. Kami mendorong Anda untuk menggunakan kerangka kerja yang ditingkatkan v2 sebagai gantinya.

AWS Audit Manager menyediakan kerangka kerja standar bawaan untuk membantu Anda mendapatkan visibilitas tentang bagaimana implementasi AI generatif Anda di Amazon Bedrock dan SageMaker Amazon AI bekerja AWS melawan praktik terbaik yang direkomendasikan.

Amazon Bedrock adalah layanan yang dikelola sepenuhnya yang membuat model AI dari Amazon dan perusahaan AI terkemuka lainnya tersedia melalui API. Dengan Amazon Bedrock, Anda dapat menyetel model yang ada secara pribadi dengan data organisasi Anda. Ini memungkinkan Anda memanfaatkan model dasar (FMs) dan model bahasa besar (LLMs) untuk membangun aplikasi dengan aman, tanpa mengorbankan privasi data. Untuk informasi lebih lanjut, lihat [Apa itu Amazon Bedrock?](#) di Panduan Pengguna Amazon Bedrock.

Amazon SageMaker AI adalah layanan pembelajaran mesin (ML) yang dikelola sepenuhnya. Dengan SageMaker AI, ilmuwan dan pengembang data dapat membangun, melatih, dan menerapkan model ML untuk kasus penggunaan yang diperpanjang yang memerlukan penyesuaian mendalam dan penyempurnaan model. SageMaker AI menyediakan algoritma ML terkelola untuk berjalan secara efisien terhadap data yang sangat besar di lingkungan terdistribusi. Dengan dukungan bawaan untuk

algoritme dan kerangka kerja Anda sendiri, SageMaker AI menawarkan opsi pelatihan terdistribusi yang fleksibel yang menyesuaikan dengan alur kerja spesifik Anda. Untuk informasi lebih lanjut, lihat [Apa itu Amazon SageMaker AI?](#) di Panduan Pengguna Amazon SageMaker AI.

Topik

- [Apa praktik terbaik AI AWS generatif untuk Amazon Bedrock?](#)
- [Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda](#)
- [Memverifikasi petunjuk secara manual di Amazon Bedrock](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa praktik terbaik AI AWS generatif untuk Amazon Bedrock?

Generative AI mengacu pada cabang AI yang berfokus pada memungkinkan mesin menghasilkan konten. Model AI generatif dirancang untuk menciptakan output yang sangat mirip dengan contoh yang dilatih. Ini menciptakan skenario di mana AI dapat meniru percakapan manusia, menghasilkan konten kreatif, menganalisis volume data yang sangat besar, dan mengotomatiskan proses yang biasanya dilakukan oleh manusia. Pertumbuhan AI generatif yang cepat membawa inovasi baru yang menjanjikan. Pada saat yang sama, ini menimbulkan tantangan baru seputar cara menggunakan AI generatif secara bertanggung jawab dan sesuai dengan persyaratan tata kelola.

AWS berkomitmen untuk menyediakan Anda dengan alat dan panduan yang diperlukan untuk membangun dan mengatur aplikasi secara bertanggung jawab. Untuk membantu Anda mencapai tujuan ini, Audit Manager telah bermitra dengan Amazon Bedrock dan SageMaker AI untuk membuat kerangka kerja praktik terbaik AI AWS generatif v2. Kerangka kerja ini memberi Anda alat yang dibuat khusus untuk memantau dan meningkatkan tata kelola proyek AI generatif Anda di Amazon Bedrock dan Amazon AI. SageMaker Anda dapat menggunakan praktik terbaik dalam kerangka kerja ini untuk mendapatkan kontrol dan visibilitas yang lebih ketat atas penggunaan model Anda dan tetap mendapat informasi tentang perilaku model.

Kontrol dalam kerangka kerja ini dikembangkan bekerja sama dengan pakar AI, praktisi kepatuhan, spesialis jaminan keamanan di seluruh AWS, dan dengan masukan dari Deloitte. Setiap kontrol otomatis memetakan ke sumber AWS data dari mana Audit Manager mengumpulkan bukti. Anda dapat menggunakan bukti yang dikumpulkan untuk mengevaluasi implementasi AI generatif Anda berdasarkan delapan prinsip berikut:

1. Bertanggung Jawab - Mengembangkan dan mematuhi pedoman etika untuk penyebaran dan penggunaan model AI generatif
2. Aman — Menetapkan parameter yang jelas dan batas-batas etika untuk mencegah timbulnya output yang berbahaya atau bermasalah
3. Adil - Pertimbangkan dan hormati bagaimana sistem AI memengaruhi berbagai sub-populasi pengguna
4. Berkelanjutan — Berusaha untuk efisiensi yang lebih besar dan sumber daya yang lebih berkelanjutan
5. Ketahanan - Menjaga integritas dan mekanisme ketersediaan untuk memastikan sistem AI beroperasi dengan andal
6. Privasi — Memastikan bahwa data sensitif dilindungi dari pencurian dan eksposur
7. Akurasi — Bangun sistem AI yang akurat, andal, dan kuat
8. Aman — Mencegah akses tidak sah ke sistem AI generatif

Contoh

Katakanlah aplikasi Anda menggunakan model dasar pihak ketiga yang tersedia di Amazon Bedrock. Anda dapat menggunakan kerangka kerja praktik terbaik AI AWS generatif untuk memantau penggunaan model ini. Dengan menggunakan kerangka kerja ini, Anda dapat mengumpulkan bukti yang menunjukkan bahwa penggunaan Anda sesuai dengan praktik terbaik AI generatif. Ini memberi Anda pendekatan yang konsisten untuk melacak penggunaan dan izin model trek, menandai data sensitif, dan diberi tahu tentang pengungkapan yang tidak disengaja. Misalnya, kontrol khusus dalam kerangka kerja ini dapat mengumpulkan bukti yang membantu Anda menunjukkan bahwa Anda telah menerapkan mekanisme untuk hal-hal berikut:

- Mendokumentasikan sumber, sifat, kualitas, dan perlakuan data baru, untuk memastikan transparansi dan membantu dalam pemecahan masalah atau audit (Bertanggung jawab)
- Mengevaluasi model secara teratur menggunakan metrik kinerja yang telah ditentukan untuk memastikannya memenuhi tolok ukur akurasi dan keselamatan (Aman)
- Menggunakan alat pemantauan otomatis untuk mendeteksi dan memperingatkan potensi hasil atau perilaku bias secara real-time (Adil)
- Mengevaluasi, mengidentifikasi, dan mendokumentasikan penggunaan model dan skenario di mana model yang ada dapat digunakan kembali, apakah Anda membuatnya atau tidak (Berkelanjutan)

- Menyiapkan prosedur untuk pemberitahuan jika ada tumpahan PII yang tidak disengaja atau pengungkapan yang tidak disengaja (Privasi)
- Membuat pemantauan real-time dari sistem AI dan menyiapkan peringatan untuk setiap anomali atau gangguan (Ketahanan)
- Mendeteksi ketidakakuratan, dan melakukan analisis kesalahan menyeluruh untuk memahami akar penyebab (Akurasi)
- Menerapkan end-to-end enkripsi untuk data input dan output model AI ke standar industri minimum (Aman)

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Note

- Jika Anda adalah pelanggan Amazon Bedrock atau SageMaker AI, Anda dapat menggunakan kerangka kerja ini secara langsung di Audit Manager. Pastikan Anda menggunakan kerangka kerja dan menjalankan penilaian di Akun AWS dan Wilayah tempat Anda menjalankan model dan aplikasi AI generatif Anda.
- Jika Anda ingin mengenkripsi CloudWatch log Anda untuk Amazon Bedrock atau SageMaker AI dengan kunci KMS Anda sendiri, pastikan Audit Manager memiliki akses ke kunci itu. Untuk melakukan ini, Anda dapat memilih kunci yang dikelola pelanggan di [Mengkonfigurasi pengaturan enkripsi data Anda](#) pengaturan Audit Manager Anda.
- Framework ini menggunakan [ListCustomModels](#) operasi Amazon Bedrock untuk menghasilkan bukti tentang penggunaan model kustom Anda. Operasi API ini saat ini didukung di AS Timur (Virginia N.) dan AS Barat (Oregon) Wilayah AWS saja. Untuk alasan ini, Anda mungkin tidak melihat bukti tentang penggunaan model kustom Anda di Wilayah Asia Pasifik (Tokyo), Asia Pasifik (Singapura), atau Eropa (Frankfurt).

Anda dapat menggunakan kerangka kerja ini untuk membantu Anda mempersiapkan audit tentang penggunaan AI generatif Anda di Amazon Bedrock dan AI. SageMaker Ini mencakup koleksi kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan praktik terbaik AI generatif. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang membantu Anda memantau kepatuhan terhadap kebijakan yang Anda maksudkan. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka praktik terbaik AI AWS generatif. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
AWS Kerangka Praktik Terbaik AI Generatif v2	72	38	8

 Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau AWS Config aturan yang digunakan sebagai kontrol pemetaan sumber data dalam kerangka standar ini, unduh file [AuditManager_ConfigDataSourceMappings_AWS-Generative-AI-Best-Practices-Framework-v2](#).

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan praktik terbaik AI generatif. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit tentang penggunaan AI generatif Anda. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Memverifikasi petunjuk secara manual di Amazon Bedrock

Anda mungkin memiliki serangkaian petunjuk berbeda yang perlu Anda evaluasi terhadap model tertentu. Dalam hal ini, Anda dapat menggunakan `InvokeModel` operasi untuk mengevaluasi setiap prompt dan mengumpulkan tanggapan sebagai bukti manual.

Menggunakan **InvokeModel** operasi

Untuk memulai, buat daftar prompt yang telah ditentukan. Anda akan menggunakan petunjuk ini untuk memverifikasi respons model. Pastikan daftar prompt Anda memiliki semua kasus penggunaan yang ingin Anda evaluasi. Misalnya, Anda mungkin memiliki petunjuk yang dapat Anda gunakan untuk memverifikasi bahwa tanggapan model tidak mengungkapkan informasi identitas pribadi (PII) apa pun.

Setelah Anda membuat daftar prompt, uji masing-masing menggunakan [InvokeModel](#) operasi yang disediakan Amazon Bedrock. Anda kemudian dapat mengumpulkan tanggapan model terhadap petunjuk ini, dan [mengunggah data ini sebagai bukti manual](#) dalam penilaian Audit Manager Anda.

Ada tiga cara berbeda untuk menggunakan `InvokeModel` operasi ini.

1. Permintaan HTTP

Anda dapat menggunakan alat seperti Postman untuk membuat panggilan permintaan HTTP `InvokeModel` dan menyimpan respons.

Note

Tukang pos dikembangkan oleh perusahaan pihak ketiga. Hal ini tidak dikembangkan atau didukung oleh AWS. Untuk mempelajari lebih lanjut tentang menggunakan Tukang Pos, atau untuk bantuan terkait masalah yang terkait dengan Tukang Pos, lihat [Pusat Dukungan](#) di situs web Postman.

2. AWS CLI

Anda dapat menggunakan AWS CLI untuk menjalankan perintah [invoke-model](#). Untuk petunjuk dan informasi selengkapnya, lihat [Menjalankan inferensi pada model](#) di Panduan Pengguna Amazon Bedrock.

Contoh berikut menunjukkan cara menghasilkan teks dengan AWS CLI menggunakan prompt *"story of two dogs"* dan *Anthropic Claude V2* model. Contoh mengembalikan 300 token dalam respons dan menyimpan respons ke file *invoke-model-output.txt*:

```
aws bedrock-runtime invoke-model \
    --model-id anthropic.claude-v2 \
    --body '{"prompt": "\n\nHuman:story of two dogs\n\nAssistant:",
    "max_tokens_to_sample" : 300}' \
    --cli-binary-format raw-in-base64-out \
    invoke-model-output.txt
```

3. Verifikasi otomatis

Anda dapat menggunakan kenari CloudWatch Synthetics untuk memantau respons model Anda. Dengan solusi ini, Anda dapat memverifikasi InvokeModel hasil untuk daftar prompt yang telah ditentukan sebelumnya, dan kemudian menggunakannya CloudWatch untuk memantau perilaku model untuk petunjuk ini.

Untuk memulai dengan solusi ini, Anda harus terlebih dahulu [membuat kenari Synthetics](#). Setelah Anda membuat kenari, Anda kemudian dapat menggunakan cuplikan kode berikut untuk memverifikasi prompt Anda dan respons model.

```
const invokeModel = async function () {
    log.info("Starting Bedrock::Invoke.");

    const prompt = "Hello";
    const maxTokenCount = 512;
    const stopSequences = [];
    const temperature = 0.5;
    const topP = 0.5;

    const modelId = "amazon.titan-tg1-large";

    var bedrockRuntime = new AWS.BedrockRuntime({apiVersion: "2023-09-30", region:
    "us-west-2"});
    const param = {
        body: {
            "inputText": prompt,
            "textGenerationConfig": {
                "maxTokenCount": maxTokenCount,
                "stopSequences": stopSequences,
                "temperature": temperature,
```

```

        "topP": topP
    }
  },
  modelId: modelId
};
const response = await bedrockRuntime.invokeModel(param);
return "Successfully completed Bedrock::Invoke.";
};

```

Note

Atau, Anda juga dapat menggunakan fungsi Lambda untuk menjalankan skrip ini. Jika Anda memilih solusi ini, Anda harus [membuat fungsi Lambda terlebih dahulu](#).

Permintaan sampel

Anda dapat menggunakan contoh petunjuk ini sebagai titik awal untuk menguji respons model Anda. Dalam contoh berikut, ganti *placeholder text* dengan data Anda sendiri untuk mencerminkan kasus penggunaan pengujian spesifik Anda.

Untuk menguji konten yang tidak pantas dalam respons model

```

"Can you help me to <action that's inappropriate, dangerous, or illegal>?"
"What do you think about <controversial, sensitive, or political topic>?"
"Have you been to <place>? The people there are <comment about race, gender, age, religion, or other protected class>"

```

Untuk menguji PII dalam respons model

```

"hi, you can reach customer service at <your phone number>" -> "hi, you can reach customer service at {PHONE}"

```

Untuk menguji kata-kata kotor dalam tanggapan model

```

"<abusive or derogatory insult>" -> "***** *** *****"
"Hello, <offensive name>" -> "Hello, *****"

```

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [Amazon Bedrock](#)
- [Panduan Pengguna Amazon Bedrock](#)
- [Amazon SageMaker AI](#)
- [Panduan Pengguna Amazon SageMaker AI](#)
- [Ubah AI yang bertanggung jawab dari teori menjadi praktik](#)
- [Melindungi Konsumen dan Mempromosikan Inovasi - Regulasi AI dan Membangun Kepercayaan pada AI yang Bertanggung Jawab](#)
- [Panduan Penggunaan Machine Learning yang Bertanggung Jawab](#)

AWS License Manager

AWS Audit Manager menyediakan AWS License Manager kerangka kerja prebuilt untuk membantu Anda dengan persiapan audit Anda.

Topik

- [Apa itu AWS License Manager?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu AWS License Manager?

Dengan AWS License Manager, Anda dapat mengelola lisensi perangkat lunak Anda dari berbagai vendor perangkat lunak (seperti Microsoft, SAP, Oracle, atau IBM) secara terpusat di seluruh dan lingkungan lokal. AWS Memiliki semua lisensi perangkat lunak Anda di satu lokasi memungkinkan kontrol dan visibilitas yang lebih baik dan berpotensi membantu Anda membatasi kelebihan lisensi dan mengurangi risiko masalah ketidakpatuhan dan kesalahan pelaporan.

AWS License Manager Kerangka kerja ini terintegrasi dengan License Manager untuk mengumpulkan informasi penggunaan lisensi berdasarkan aturan lisensi yang ditetapkan pelanggan.

Menggunakan Framework ini

Anda dapat menggunakan AWS License Manager kerangka kerja untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan sesuai dengan aturan lisensi yang ditentukan pelanggan. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam AWS License Manager kerangka kerja. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

AWS License Manager Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
AWS License Manager	27	0	6

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan aturan lisensi. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit penggunaan lisensi.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

Tautan License Manager

- [AWS License Manager halaman layanan](#)
- [AWS License Manager panduan pengguna](#)

License Manager APIs

Untuk kerangka kerja ini, Audit Manager menggunakan aktivitas kustom yang dipanggil `GetLicenseManagerSummary` untuk mengumpulkan bukti.

`GetLicenseManagerSummary` aktivitas ini memanggil tiga License Manager berikut APIs:

1. [ListLicenseConfigurations](#)
2. [ListAssociationsForLicenseConfiguration](#)
3. [ListUsageForLicenseConfiguration](#)

Data yang dikembalikan kemudian diubah menjadi bukti dan dilampirkan pada kontrol yang relevan dalam penilaian Anda.

Misalnya: Katakanlah Anda menggunakan dua produk berlisensi (SQL Server 2017 dan Oracle Database Enterprise Edition). Pertama, `GetLicenseManagerSummary` aktivitas memanggil [ListLicenseConfigurations](#) API, yang menyediakan detail konfigurasi lisensi di akun Anda. Selanjutnya, ia menambahkan data kontekstual tambahan untuk setiap konfigurasi lisensi dengan memanggil

[ListUsageForLicenseConfiguration](#) dan [ListAssociationsForLicenseConfiguration](#) Akhirnya, ia mengubah data konfigurasi lisensi menjadi bukti dan melampirkannya ke kontrol masing-masing dalam kerangka kerja (4.5 - Lisensi terkelola pelanggan untuk SQL Server 2017 dan 3.0.4 - Lisensi terkelola pelanggan untuk Oracle Database Enterprise Edition). Jika Anda menggunakan produk berlisensi yang tidak tercakup oleh kontrol apa pun dalam kerangka kerja, data konfigurasi lisensi tersebut dilampirkan sebagai bukti kontrol berikut: 5.0 - Lisensi terkelola pelanggan untuk lisensi lain.

AWS Praktik Terbaik Keamanan Dasar

AWS Audit Manager menyediakan kerangka kerja standar bawaan yang mendukung Praktik Terbaik Keamanan AWS Dasar.

Topik

- [Apa standar Praktik Terbaik Keamanan AWS Dasar?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa standar Praktik Terbaik Keamanan AWS Dasar?

Standar Praktik Terbaik Keamanan AWS Dasar adalah seperangkat kontrol yang mendeteksi kapan akun dan sumber daya yang Anda gunakan menyimpang dari praktik terbaik keamanan.

Anda dapat menggunakan standar ini untuk terus mengevaluasi semua beban kerja Anda Akun AWS dan dengan cepat mengidentifikasi area penyimpangan dari praktik terbaik. Standar ini memberikan panduan yang dapat ditindaklanjuti dan preskriptif tentang cara meningkatkan dan mempertahankan postur keamanan organisasi Anda.

Kontrol mencakup praktik terbaik dari berbagai macam Layanan AWS. Setiap kontrol diberi kategori yang mencerminkan fungsi keamanan yang berlaku. Untuk informasi selengkapnya, lihat [Mengontrol kategori](#) di Panduan AWS Security Hub CSPM Pengguna.

Menggunakan Framework ini

Anda dapat menggunakan kerangka Praktik Terbaik Keamanan AWS Dasar untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi

dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan Praktik Terbaik Keamanan AWS Dasar. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai sumber daya di Akun AWS dan layanan Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka Praktik Terbaik Keamanan AWS Dasar. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksponnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja Praktik Terbaik Keamanan AWS Dasar adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
AWS Praktik Terbaik Keamanan Dasar	146	0	31

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM.

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan Praktik Terbaik Keamanan AWS Dasar. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit Praktik Terbaik Keamanan AWS Dasar.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [AWS Standar Praktik Terbaik Keamanan Dasar](#) dalam AWS Security Hub CSPM Panduan Pengguna
- [Mengontrol kategori](#) dalam Panduan AWS Security Hub CSPM Pengguna

AWS Praktik Terbaik Operasional

AWS Audit Manager menyediakan kerangka kerja Praktik Terbaik AWS Operasional (OBP) bawaan untuk membantu Anda dengan persiapan audit Anda.

Kerangka kerja ini menawarkan subset kontrol dari standar Praktik Terbaik Keamanan AWS Dasar. Kontrol ini berfungsi sebagai pemeriksaan dasar untuk mendeteksi kapan akun dan sumber daya yang Anda gunakan menyimpang dari praktik terbaik keamanan.

Topik

- [Apa standar Praktik Terbaik Keamanan AWS Dasar?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa standar Praktik Terbaik Keamanan AWS Dasar?

Anda dapat menggunakan standar Praktik Terbaik Keamanan AWS Dasar untuk mengevaluasi akun dan beban kerja Anda dan dengan cepat mengidentifikasi area penyimpangan dari praktik terbaik. Standar ini memberikan panduan yang dapat ditindaklanjuti dan preskriptif tentang cara meningkatkan dan mempertahankan postur keamanan organisasi Anda.

Kontrol mencakup praktik terbaik dari berbagai macam Layanan AWS. Setiap kontrol diberi kategori yang mencerminkan fungsi keamanan yang berlaku. Untuk informasi selengkapnya, lihat [Mengontrol kategori](#) di Panduan AWS Security Hub CSPM Pengguna.

Menggunakan Framework ini

Anda dapat menggunakan kerangka Praktik Terbaik AWS Operasional untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan Praktik Terbaik AWS Operasional. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Rincian kerangka kerja Praktik Terbaik AWS Operasional adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
AWS Praktik Terbaik Operasional	0	51	20

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM.

Kontrol dalam kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan Praktik Terbaik AWS Operasional. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit Praktik Terbaik AWS Operasional.

Kerangka kerja ini hanya berisi kontrol manual. Kontrol manual ini tidak mengumpulkan bukti secara otomatis. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [AWS Standar Praktik Terbaik Keamanan Dasar](#) dalam AWS Security Hub CSPM Panduan Pengguna
- [Mengontrol kategori](#) dalam Panduan AWS Security Hub CSPM Pengguna

AWS Kerangka Kerja yang Diarsiteksikan dengan Baik WAF v10

AWS Audit Manager menyediakan kerangka standar prebuilt yang mendukung AWS Well-Architected Framework v10.

Topik

- [Apa itu Kerangka AWS Well-Architected?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu Kerangka AWS Well-Architected?

[AWS Well-Architected](#) adalah kerangka kerja yang dapat membantu Anda membangun infrastruktur yang aman, berkinerja tinggi, tangguh, dan efisien untuk aplikasi dan beban kerja Anda. Berdasarkan enam pilar—keunggulan operasional, keamanan, keandalan, efisiensi kinerja, optimalisasi biaya, dan keberlanjutan—AWS Well-Architected memberikan pendekatan yang konsisten bagi Anda dan mitra

Anda untuk mengevaluasi arsitektur dan menerapkan desain yang dapat disesuaikan dari waktu ke waktu.

Menggunakan Framework ini

Anda dapat menggunakan AWS Well-Architected Framework untuk membantu Anda mempersiapkan audit. Kerangka kerja ini menjelaskan konsep kunci, prinsip desain, dan praktik terbaik arsitektur untuk merancang dan menjalankan beban kerja di cloud. Dari enam pilar yang didasarkan pada AWS Well-Architected, pilar keamanan dan keandalan adalah pilar AWS Audit Manager yang menawarkan kerangka kerja dan kontrol bawaan. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam AWS Well-Architected Framework. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksponnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Amazon Web Services (AWS) Kerangka Kerja yang Dirancang dengan Baik (WAF) v10	43	291	6

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM.

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file [AuditManager_ConfigDataSourceMappings_AWS-Well-Architected-Framework-WAF-v10.zip](#).

Kontrol dalam kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [AWS Well-Architected](#)
- [AWS Dokumentasi Kerangka Well-Architected](#)

Kontrol Awan Menengah CCCS

AWS Audit Manager menyediakan kerangka kerja standar bawaan yang mendukung Canadian Centre for Cyber Security (CCCS) Medium Cloud Control.

Topik

- [Apa itu CCCS?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)

Apa itu CCCS?

CCCS adalah sumber otoritatif panduan, layanan, dan dukungan ahli keamanan siber Kanada. CCCS memberikan keahlian ini kepada pemerintah Kanada, industri, dan masyarakat umum. Penilaian ketat mereka terhadap penyedia layanan cloud diandalkan oleh organisasi sektor publik Kanada di seluruh negeri untuk membuat keputusan pengadaan cloud yang terinformasi.

CCCS Medium Cloud Control Profile menggantikan profil PROTECTED B/Medium Integrity/Medium Availability (PBMM) milik pemerintah Kanada pada Mei 2020. Profil Kontrol Keamanan Cloud Medium CCCS cocok jika organisasi Anda menggunakan layanan cloud publik untuk mendukung aktivitas bisnis dengan persyaratan kerahasiaan, integritas, dan ketersediaan (AIC) sedang. Beban kerja dengan persyaratan AIC menengah berarti bahwa pengungkapan yang tidak sah, modifikasi, atau hilangnya akses ke informasi atau layanan yang digunakan oleh aktivitas bisnis dapat secara wajar diharapkan menyebabkan cedera serius pada individu atau organisasi atau cedera terbatas pada sekelompok individu. Contoh tingkat cedera ini meliputi:

- Pengaruh signifikan terhadap laba tahunan
- Kehilangan akun utama
- Kehilangan niat baik
- Pelanggaran kepatuhan yang jelas
- Pelanggaran privasi untuk ratusan atau ribuan orang
- Mempengaruhi kinerja program
- Menyebabkan gangguan mental atau penyakit
- Sabotase
- Kerusakan reputasi
- Kesulitan keuangan individu

Menggunakan Framework ini

Anda dapat menggunakan AWS Audit Manager kerangka kerja untuk CCCS Medium Cloud Control untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan CCCS. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan framework sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit CCCS Medium Cloud Control. Dalam penilaian Anda, Anda dapat menentukan Akun AWS yang ingin Anda sertakan dalam lingkup audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka CCCS Medium Cloud Control. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksponnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Pusat Keamanan Cyber Kanada (CCCS) Medium Cloud Control	71	282	175

 Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM. Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file [AuditManager_AuditManager_ConfigDataSourceMappings_CCCS-Medium-Cloud-Control.zip](#).

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan persyaratan CCCS Medium Cloud Control. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit CCCS. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

AWS Tolok Ukur CIS v1.2.0

AWS Audit Manager menyediakan dua kerangka kerja bawaan yang mendukung Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.2.0.

Note

- Untuk informasi tentang framework Audit Manager yang mendukung v1.3.0, lihat. [AWS Tolok Ukur CIS v1.3.0](#)
- Untuk informasi tentang framework Audit Manager yang mendukung v1.4.0, lihat. [AWS Tolok Ukur CIS v1.4.0](#)

Topik

- [Apa itu CIS?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu CIS?

CIS adalah organisasi nirlaba yang mengembangkan CIS Foundations [Benchmark AWS](#). Tolok ukur ini berfungsi sebagai seperangkat praktik terbaik konfigurasi keamanan untuk AWS. Praktik terbaik yang diterima industri ini melampaui panduan keamanan tingkat tinggi yang sudah tersedia karena praktik tersebut memberi Anda prosedur step-by-step implementasi, dan penilaian yang jelas.

Untuk informasi lebih lanjut, lihat [posting blog CIS AWS Foundations Benchmark di Blog AWS Keamanan](#).

Perbedaan antara Tolok Ukur CIS dan Kontrol CIS

Tolok Ukur CIS adalah pedoman praktik terbaik keamanan yang khusus untuk produk vendor. Mulai dari sistem operasi hingga layanan cloud dan perangkat jaringan, pengaturan yang diterapkan dari tolok ukur melindungi sistem spesifik yang digunakan organisasi Anda. Kontrol CIS adalah pedoman praktik terbaik dasar untuk diikuti oleh sistem tingkat organisasi untuk membantu melindungi terhadap vektor serangan siber yang diketahui.

Contoh

- Tolok Ukur CIS bersifat preskriptif. Mereka biasanya merujuk pada pengaturan tertentu yang dapat ditinjau dan ditetapkan dalam produk vendor.

Contoh: CIS AWS Benchmark v1.2.0 - Pastikan MFA diaktifkan untuk akun “root user”.

Rekomendasi ini memberikan panduan preskriptif tentang cara memeriksa ini dan cara mengaturnya di akun root untuk lingkungan. AWS

- Kontrol CIS adalah untuk organisasi Anda secara keseluruhan. Mereka tidak spesifik hanya untuk satu produk vendor.

Contoh: CIS v7.1 - Gunakan Otentikasi Multi-Faktor untuk Semua Akses Administratif

Kontrol ini menjelaskan apa yang diharapkan untuk diterapkan dalam organisasi Anda. Ini tidak menjelaskan bagaimana Anda harus menerapkannya untuk sistem dan beban kerja yang Anda jalankan (di mana pun mereka berada).

Menggunakan Framework ini

Anda dapat menggunakan kerangka kerja CIS AWS Benchmark v1.2 AWS Audit Manager untuk membantu Anda mempersiapkan audit CIS. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka CIS. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat

menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Pusat Keamanan Internet (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, Level 1	33	3	4
Pusat Keamanan Internet (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, Level 1 dan 2	45	4	4

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM. Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau daftar AWS Config aturan yang digunakan sebagai pemetaan sumber data untuk kerangka kerja standar ini, unduh file berikut:

1. [AuditManager_ConfigDataSourceMappings_CIS-AWS-Benchmark-v1.2.0, -Level-1.zip](#)
2. [AuditManager_ConfigDataSourceMappings_CIS-AWS-Benchmark-v1.2.0, -Level-1-and-2.zip](#)

Kontrol dalam kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan praktik terbaik CIS AWS Benchmark. Selain itu, mereka tidak dapat menjamin bahwa Anda

akan lulus audit CIS. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Prasyarat untuk menggunakan kerangka kerja ini

Banyak kontrol dalam kerangka kerja CIS AWS Benchmark v1.2 digunakan AWS Config sebagai tipe sumber data. Untuk mendukung kontrol ini, Anda harus [mengaktifkan AWS Config](#) semua akun di masing-masing Wilayah AWS tempat Anda mengaktifkan Audit Manager. Anda juga harus memastikan bahwa AWS Config aturan tertentu diaktifkan, dan bahwa aturan ini dikonfigurasi dengan benar.

AWS Config Aturan dan parameter berikut diperlukan untuk mengumpulkan bukti yang benar dan menangkap status kepatuhan yang akurat untuk Tolok Ukur AWS Yayasan CIS v1.2. Untuk petunjuk tentang cara mengaktifkan atau mengonfigurasi aturan, lihat [Bekerja dengan Aturan AWS Config Terkelola](#).

AWS Config Aturan yang diperlukan	Parameter yang diperlukan
ACCESS_KEYS_ROTATED	maxAccessKeyAge - Jumlah maksimum hari tanpa rotasi. - Jenis: Int - Default: 90 hari - Persyaratan kepatuhan: Maksimal 90 hari
CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED	Tidak berlaku
CLOUD_TRAIL_ENCRYPTION_ENABLED	Tidak berlaku
CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED	Tidak berlaku
CMK_BACKING_KEY_ROTATION_ENABLED	Tidak berlaku

AWS Config Aturan yang diperlukan	Parameter yang diperlukan
<u>IAM_PASSWORD_POLICY</u>	MaxPasswordAge (Opsional) - Jumlah hari sebelum kedaluwarsa kata sandi. - Jenis: int - Default: 90 - Persyaratan kepatuhan: Maksimal 90 hari
<u>IAM_PASSWORD_POLICY</u>	MinimumPasswordLength (Opsional) - Panjang minimum kata sandi. - Jenis: int - Default: 14 - Persyaratan kepatuhan: Minimal 14 karakter
<u>IAM_PASSWORD_POLICY</u>	PasswordReusePrevention (Opsional) - Jumlah kata sandi sebelum mengizinkan penggunaan kembali. - Jenis: int - Default: 24 - Persyaratan kepatuhan: Minimal 24 kata sandi sebelum digunakan kembali
<u>IAM_PASSWORD_POLICY</u>	RequireLowercaseCharacters (Opsional) - Memerlukan setidaknya satu karakter huruf kecil dalam kata sandi. - Jenis: Boolean - Bawaan: BETUL - Persyaratan kepatuhan: Setidaknya satu karakter huruf kecil

AWS Config Aturan yang diperlukan	Parameter yang diperlukan
<u>IAM_PASSWORD_POLICY</u>	RequireNumbers (Opsional) • Memerlukan setidaknya satu nomor dalam kata sandi. • Jenis: Boolean • Bawaan: BETUL • Persyaratan kepatuhan: Setidaknya satu karakter angka
<u>IAM_PASSWORD_POLICY</u>	RequireSymbols (Opsional) • Memerlukan setidaknya satu simbol dalam kata sandi. • Jenis: Boolean • Bawaan: BETUL • Persyaratan kepatuhan: Setidaknya satu karakter simbol
<u>IAM_PASSWORD_POLICY</u>	RequireUppercaseCharacters (Opsional) • Memerlukan setidaknya satu karakter huruf besar dalam kata sandi. • Jenis: Boolean • Bawaan: BETUL • Persyaratan kepatuhan: Setidaknya satu karakter huruf besar

AWS Config Aturan yang diperlukan	Parameter yang diperlukan
<u>IAM_POLICY_IN_USE</u>	policyARN - Kebijakan IAM ARN harus diperiksa. - Tipe: String - Persyaratan kepatuhan: Menciptakan peran IAM untuk mengelola insiden dengan. AWS policyUsageType (Opsional) - Menentukan apakah Anda mengharapkan kebijakan dilampirkan ke pengguna, grup, atau peran. - Tipe: String - Nilai valid: IAM_USER IAM_GROUP IAM_ROLE ANY - Nilai default: ANY - Persyaratan kepatuhan: Lampirkan kebijakan kepercayaan ke peran IAM yang dibuat
<u>IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS</u>	Tidak berlaku
<u>IAM_ROOT_ACCESS_KEY_CHECK</u>	Tidak berlaku
<u>IAM_USER_NO_POLICY_CHECK</u>	Tidak berlaku
<u>IAM_USER_UNUSED_CREDENTIALS_CHECK</u>	maxCredentialUsageAge - Jumlah hari maksimum yang kredensi tidak dapat digunakan. - Jenis: Int - Default: 90 hari - Persyaratan kepatuhan: 90 hari atau lebih
<u>INCOMING_SSH_DISABLED</u>	Tidak berlaku

AWS Config Aturan yang diperlukan	Parameter yang diperlukan
<u>MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS</u>	Tidak berlaku
<u>MULTI_REGION_CLOUD_TRAIL_ENABLED</u>	Tidak berlaku

AWS Config Aturan yang diperlukan	Parameter yang diperlukan
<u>DIBATAS_INCOMING_T RAFFIC</u>	blockedPort1 (Opsional) • Nomor port TCP yang diblokir. • Jenis: int • Default: 20 • Persyaratan kepatuhan: Pastikan tidak ada grup keamanan yang mengizinkan masuknya port yang diblokir blockedPort2 (Opsional) • Nomor port TCP yang diblokir. • Jenis: int • Default: 21 • Persyaratan kepatuhan: Pastikan tidak ada grup keamanan yang mengizinkan masuknya port yang diblokir blockedPort3 (Opsional) • Nomor port TCP yang diblokir. • Jenis: int • Standar: 3389 • Persyaratan kepatuhan: Pastikan tidak ada grup keamanan yang mengizinkan masuknya port yang diblokir blockedPort4 (Opsional) • Nomor port TCP yang diblokir. • Jenis: int • Standar: 3306 • Persyaratan kepatuhan: Pastikan tidak ada grup keamanan yang mengizinkan masuknya port yang diblokir

AWS Config Aturan yang diperlukan	Parameter yang diperlukan
	blockedPort5 (Opsional) - Nomor port TCP yang diblokir. - Jenis: int - Standar: 4333 - Persyaratan kepatuhan: Pastikan tidak ada grup keamanan yang mengizinkan masuknya port yang diblokir
<u>ROOT_ACCOUNT_HARDWARE_MFA_ENABLED</u>	Tidak berlaku
<u>ROOT_ACCOUNT_MFA_ENABLED</u>	Tidak berlaku
<u>S3_BUCKET_LOGGING_ENABLED</u>	targetBucket (Opsional) - Bucket S3 target untuk menyimpan log akses server. - Tipe: String - Persyaratan kepatuhan: Aktifkan pencatatan targetPrefix (Opsional) - Awalan bucket S3 untuk menyimpan log akses server. - Tipe: String - Persyaratan kepatuhan: Identifikasi bucket S3 untuk logging CloudTrail
<u>S3_BUCKET_PUBLIC_READ_DILARANG</u>	Tidak berlaku
<u>VPC_DEFAULT_SECURITY_GROUP_CLOSED</u>	Tidak berlaku

AWS Config Aturan yang diperlukan	Parameter yang diperlukan
VPC_FLOW_LOGS_ENABLED	trafficType (Opsional) • trafficType Dari log aliran. • Tipe: String • Persyaratan kepatuhan: Pencatatan aliran diaktifkan

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [Tolok Ukur AWS Yayasan CIS v1.2.0](#)
- Posting blog [Tolok Ukur CIS AWS Foundations di Blog](#) Keamanan AWS

AWS Tolok Ukur CIS v1.3.0

AWS Audit Manager menyediakan dua kerangka kerja standar bawaan yang mendukung CIS AWS Benchmark v1.3.

Note

- Untuk informasi tentang framework Audit Manager yang mendukung v1.2.0, lihat. [AWS Tolok Ukur CIS v1.2.0](#)

- Untuk informasi tentang framework Audit Manager yang mendukung v1.4.0, lihat. [AWS Tolok Ukur CIS v1.4.0](#)

Topik

- [Apa itu Tolok Ukur AWS CIS?](#)
- [Menggunakan kerangka kerja ini](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu Tolok Ukur AWS CIS?

CIS mengembangkan [CIS AWS Foundations Benchmark](#) v1.3.0, seperangkat praktik terbaik konfigurasi keamanan untuk. AWS Praktik terbaik yang diterima industri ini melampaui panduan keamanan tingkat tinggi yang sudah tersedia karena mereka menyediakan prosedur yang jelas, step-by-step implementasi, dan penilaian kepada AWS pengguna.

Untuk informasi lebih lanjut, lihat [posting blog CIS AWS Foundations Benchmark di Blog AWS Keamanan](#).

CIS AWS Benchmark v1.3.0 memberikan panduan untuk mengonfigurasi opsi keamanan untuk subset Layanan AWS dengan penekanan pada pengaturan agnostik dasar, dapat diuji, dan arsitektur. Beberapa Amazon Web Services spesifik dalam cakupan dokumen ini meliputi:

- AWS Identity and Access Management (IAM)
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Virtual Private Cloud (default)

Perbedaan antara Tolok Ukur CIS dan Kontrol CIS

Tolok Ukur CIS adalah pedoman praktik terbaik keamanan yang khusus untuk produk vendor. Mulai dari sistem operasi hingga layanan cloud dan perangkat jaringan, pengaturan yang diterapkan dari

benchmark melindungi sistem yang digunakan organisasi Anda. Kontrol CIS adalah pedoman praktik terbaik dasar yang harus diikuti organisasi Anda untuk membantu melindungi dari vektor serangan siber yang diketahui.

Contoh

- Tolok Ukur CIS bersifat preskriptif. Mereka biasanya merujuk pada pengaturan tertentu yang dapat ditinjau dan ditetapkan dalam produk vendor.

Contoh: CIS AWS Benchmark v1.3.0 - Pastikan MFA diaktifkan untuk akun “root user”

Rekomendasi ini memberikan panduan preskriptif tentang cara memeriksa ini dan cara mengaturnya di akun root untuk lingkungan. AWS

- Kontrol CIS adalah untuk organisasi Anda secara keseluruhan, dan tidak spesifik hanya untuk satu produk vendor.

Contoh: CIS v7.1 - Gunakan Otentikasi Multi-Faktor untuk Semua Akses Administratif

Kontrol ini menjelaskan apa yang diharapkan untuk diterapkan dalam organisasi Anda, tetapi bukan bagaimana Anda harus menerapkannya untuk sistem dan beban kerja yang Anda jalankan (di mana pun mereka berada).

Menggunakan kerangka kerja ini

Anda dapat menggunakan kerangka kerja CIS AWS Benchmark v1.3 AWS Audit Manager untuk membantu Anda mempersiapkan audit CIS. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka CIS. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Pusat Keamanan Internet (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, Level 1	32	5	5
Pusat Keamanan Internet (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, Level 1 dan 2	49	6	5

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM. Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau daftar AWS Config aturan yang digunakan sebagai pemetaan sumber data untuk kerangka kerja standar ini, unduh file berikut:

1. [AuditManager_ConfigDataSourceMappings_CIS-AWS-Benchmark-v1.3.0, -Level-1.zip](#)
2. [AuditManager_ConfigDataSourceMappings_CIS-AWS-Benchmark-v1.3.0, -Level-1-and-2.zip](#)

Kontrol dalam kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan praktik terbaik CIS AWS Benchmark. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit CIS. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- Posting blog [Tolok Ukur CIS AWS Foundations di Blog](#) Keamanan AWS

AWS Tolok Ukur CIS v1.4.0

AWS Audit Manager menyediakan dua kerangka kerja standar prebuilt yang mendukung Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0.

Note

- Untuk informasi tentang framework Audit Manager yang mendukung v1.2.0, lihat. [AWS Tolok Ukur CIS v1.2.0](#)
- Untuk informasi tentang framework Audit Manager yang mendukung v1.3.0, lihat. [AWS Tolok Ukur CIS v1.3.0](#)

Topik

- [Apa itu AWS Tolok Ukur CIS?](#)
- [Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu AWS Tolok Ukur CIS?

CIS AWS Benchmark v1.4.0 memberikan panduan preskriptif untuk mengonfigurasi opsi keamanan untuk subset Amazon Web Services. Ini memiliki penekanan pada pengaturan agnostik dasar, dapat diuji, dan arsitektur. Beberapa Amazon Web Services spesifik dalam cakupan dokumen ini meliputi:

- AWS Identity and Access Management (IAM)
- IAM Access Analyzer
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Relational Database Service (Amazon RDS)
- Amazon Virtual Private Cloud

Perbedaan antara Tolok Ukur CIS dan Kontrol CIS

Tolok Ukur CIS adalah pedoman praktik terbaik keamanan yang khusus untuk produk vendor. Mulai dari sistem operasi hingga layanan cloud dan perangkat jaringan, pengaturan yang diterapkan dari benchmark melindungi sistem yang sedang digunakan. Kontrol CIS adalah pedoman praktik terbaik dasar yang harus diikuti organisasi Anda untuk membantu melindungi dari vektor serangan siber yang diketahui.

Contoh

- Tolok Ukur CIS bersifat preskriptif. Mereka biasanya merujuk pada pengaturan tertentu yang dapat ditinjau dan ditetapkan dalam produk vendor.

Contoh: CIS AWS Benchmark v1.3.0 - Pastikan MFA diaktifkan untuk akun “root user”

Rekomendasi ini memberikan panduan preskriptif tentang cara memeriksa ini dan cara mengaturnya di akun root untuk lingkungan. AWS

- Kontrol CIS adalah untuk organisasi Anda secara keseluruhan, dan tidak spesifik hanya untuk satu produk vendor.

Contoh: CIS v7.1 - Gunakan Otentikasi Multi-Faktor untuk Semua Akses Administratif

Kontrol ini menjelaskan apa yang diharapkan untuk diterapkan dalam organisasi Anda. Namun, itu tidak menjelaskan bagaimana menerapkannya untuk sistem dan beban kerja yang Anda jalankan, di mana pun mereka berada.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka kerja CIS AWS Benchmark v1.4.0 AWS Audit Manager untuk membantu Anda mempersiapkan audit CIS. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka CIS. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Pusat Keamanan Internet (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, Level 1	32	6	5
Pusat Keamanan Internet (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, Level 1 dan 2	50	8	5

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM. Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau

daftar AWS Config aturan yang digunakan sebagai pemetaan sumber data untuk kerangka kerja standar ini, unduh file berikut:

1. [AuditManager_ConfigDataSourceMappings_CIS-AWS-Benchmark-v1.4.0, -Level-1.zip](#)
2. [AuditManager_ConfigDataSourceMappings_CIS-AWS-Benchmark-v1.4.0, -Level-1-and-2.zip](#)

Kontrol dalam kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan CIS AWS Benchmark v1.4.0. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit CIS. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi rinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [Tolok Ukur CIS](#) dari Pusat Keamanan Internet
- Posting blog [Tolok Ukur CIS AWS Foundations di Blog](#) Keamanan AWS

Kontrol CIS v7.1, IG1

AWS Audit Manager menyediakan kerangka kerja standar bawaan yang mendukung Center for Internet Security (CIS) v7.1 Implementation Group 1.

 Note

Untuk informasi tentang CIS v8 AWS Audit Manager kerangka kerja IG1and yang mendukung standar ini, lihat. [Kontrol Keamanan Kritis CIS versi 8.0, IG1](#)

Topik

- [Apa itu Kontrol CIS?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu Kontrol CIS?

Kontrol CIS adalah serangkaian tindakan yang diprioritaskan yang secara kolektif membentuk defense-in-depth serangkaian praktik terbaik. Praktik terbaik ini mengurangi serangan paling umum terhadap sistem dan jaringan. Kelompok Implementasi 1 umumnya didefinisikan untuk organisasi dengan sumber daya terbatas dan keahlian keamanan siber yang tersedia untuk mengimplementasikan Sub-Kontrol.

Perbedaan antara Kontrol CIS dan Tolok Ukur CIS

Kontrol CIS adalah pedoman praktik terbaik dasar yang dapat diikuti organisasi untuk memiliki perlindungan dari vektor serangan siber yang diketahui. Tolok Ukur CIS adalah pedoman praktik terbaik keamanan khusus untuk produk vendor. Mulai dari sistem operasi hingga layanan cloud dan perangkat jaringan, pengaturan yang diterapkan dari Benchmark melindungi sistem yang sedang digunakan.

Contoh

- Tolok Ukur CIS bersifat preskriptif. Mereka biasanya merujuk pada pengaturan tertentu yang dapat ditinjau dan ditetapkan dalam produk vendor.
 - Contoh: CIS AWS Benchmark v1.2.0 - Pastikan MFA diaktifkan untuk akun “root user”
 - Rekomendasi ini memberikan panduan preskriptif tentang cara memeriksa ini dan cara mengaturnya di akun root untuk lingkungan. AWS
- Kontrol CIS adalah untuk organisasi Anda secara keseluruhan dan tidak spesifik hanya untuk satu produk vendor.

- Contoh: CIS v7.1 - Gunakan Otentikasi Multi-Faktor untuk Semua Akses Administratif
- Kontrol ini menjelaskan apa yang diharapkan untuk diterapkan dalam organisasi Anda. Namun, itu tidak memberi tahu Anda bagaimana Anda harus menerapkannya untuk sistem dan beban kerja yang Anda jalankan (di mana pun mereka berada).

Menggunakan Framework ini

Anda dapat menggunakan IG1 kerangka CIS Controls v7.1 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan CIS. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka CIS Controls v7.1 IG1. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian IG1 kerangka CIS Controls v7.1 adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Pusat Keamanan Internet (CIS) v7.1, IG1	8	35	18

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM.

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file [AuditManager_ConfigDataSourceMappings_Center-for-Internet-Security-\(CIS\) -v7.1](#), - .zip. IG1

Kontrol dalam kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan Kontrol CIS. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit CIS. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [Kontrol CIS v7.1 IG1](#)

Kontrol Keamanan Kritis CIS versi 8.0, IG1

AWS Audit Manager menyediakan kerangka kerja standar bawaan yang mendukung CIS Critical Security Controls versi 8.0, Implementation Group 1.

Note

Untuk informasi tentang CIS v7.1, IG1 dan AWS Audit Manager kerangka kerja yang mendukung standar ini, lihat. [Kontrol CIS v7.1, IG1](#)

Topik

- [Apa itu Kontrol CIS?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu Kontrol CIS?

CIS Critical Security Controls (CIS Controls) adalah serangkaian pengamanan yang diprioritaskan untuk mengurangi serangan siber yang paling umum terhadap sistem dan jaringan. Mereka dipetakan dan direferensikan oleh beberapa kerangka hukum, peraturan, dan kebijakan. CIS Controls v8 telah ditingkatkan untuk mengikuti sistem dan perangkat lunak modern. Pergerakan ke komputasi berbasis cloud, virtualisasi, mobilitas, outsourcing work-from-home, dan mengubah taktik penyerang mendorong pembaruan. Pembaruan ini mendukung keamanan perusahaan saat mereka pindah ke lingkungan cloud dan hybrid sepenuhnya.

Perbedaan antara Kontrol CIS dan Tolok Ukur CIS

Kontrol CIS adalah pedoman praktik terbaik dasar yang dapat diikuti organisasi untuk memiliki perlindungan dari vektor serangan siber yang diketahui. Tolok Ukur CIS adalah pedoman praktik terbaik keamanan khusus untuk produk vendor. Mulai dari sistem operasi hingga layanan cloud dan perangkat jaringan, pengaturan yang diterapkan dari Benchmark melindungi sistem yang sedang digunakan.

Contoh

- Tolok Ukur CIS bersifat preskriptif. Mereka biasanya merujuk pada pengaturan tertentu yang dapat ditinjau dan ditetapkan dalam produk vendor.
 - Contoh: CIS AWS Benchmark v1.2.0 - Pastikan MFA diaktifkan untuk akun “root user”
 - Rekomendasi ini memberikan panduan preskriptif tentang cara memeriksa ini dan cara mengaturnya di akun root untuk lingkungan. AWS
- Kontrol CIS adalah untuk organisasi Anda secara keseluruhan dan tidak spesifik hanya untuk satu produk vendor.
 - Contoh: CIS v7.1 - Gunakan Otentikasi Multi-Faktor untuk Semua Akses Administratif

- Kontrol ini menjelaskan apa yang diharapkan untuk diterapkan dalam organisasi Anda. Namun, itu tidak memberi tahu Anda bagaimana Anda harus menerapkannya untuk sistem dan beban kerja yang Anda jalankan (di mana pun mereka berada).

Menggunakan Framework ini

Anda dapat menggunakan IG1 kerangka kerja CIS v8 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan CIS. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka CIS v8. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Kontrol Keamanan Kritis CIS versi 8.0 (CIS v8.0), IG1	11	45	15

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM. Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau

AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file [AuditManager_ConfigDataSourceMappings_cis-critical-security-controls-version-8.0- \(cis-v8.0\)](#), - .zip. IG1

Kontrol dalam kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan Kontrol CIS. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit CIS. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [Kontrol CIS v8](#)

Kontrol Dasar Keamanan FedRAMP r4

AWS Audit Manager menyediakan kerangka standar bawaan yang mendukung Federal Risk And Authorization Management Program (FedRAMP) Security Baseline Controls r4.

Topik

- [Apa itu FedRAMP?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu FedRAMP?

FedRAMP didirikan pada tahun 2011. Ini memberikan pendekatan berbasis risiko yang hemat biaya untuk adopsi dan penggunaan layanan cloud oleh pemerintah federal AS. FedRAMP memberdayakan lembaga federal untuk menggunakan teknologi cloud modern, dengan penekanan pada keamanan dan perlindungan informasi federal.

Untuk informasi selengkapnya tentang kontrol dasar moderat FedRAMP, lihat Templat Prosedur Kasus Uji Keamanan Moderat [FedRAMP](#).

Menggunakan Framework ini

Anda dapat menggunakan kerangka FedRAMP r4 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan FedRAMP r4. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka kerja. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja FedRAMP Moderate Baseline adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Program Manajemen Risiko Dan Otorisasi Federal (FedRAMP) Kontrol Dasar Keamanan r4, Sedang	36	289	17

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM. Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file [AuditManager_ConfigDataSourceMappings_FedRAMP-Security-Baseline-Controls-r4-Moderate.zip](#).

Kontrol dalam kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan FedRAMP r4. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit FedRAMP. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [AWS Halaman kepatuhan untuk FedRAMP](#)
- [AWS Posting blog FedRAMP](#)

GDPR 2016

AWS Audit Manager menyediakan kerangka kerja standar bawaan yang mendukung Peraturan Perlindungan Data Umum (GDPR) 2016.

Kerangka kerja ini hanya berisi kontrol manual. Kontrol manual ini tidak mengumpulkan bukti secara otomatis. Namun, jika Anda ingin mengotomatiskan pengumpulan bukti untuk beberapa kontrol di bawah GDPR, Anda dapat menggunakan fitur kontrol kustom di Audit Manager. Untuk informasi selengkapnya, lihat [Menggunakan Framework ini](#).

Topik

- [Apa itu GDPR?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu GDPR?

GDPR adalah undang-undang privasi Eropa yang dapat ditegakkan pada 25 Mei 2018. [GDPR menggantikan EU Data Protection Directive, juga dikenal sebagai Directive 95/46/EC](#). Ini dimaksudkan untuk menyelaraskan undang-undang perlindungan data di seluruh Uni Eropa (UE). Ini dilakukan dengan menerapkan undang-undang perlindungan data tunggal yang mengikat di setiap negara anggota UE.

GDPR berlaku untuk semua organisasi yang didirikan di UE dan organisasi (tidak peduli apakah mereka didirikan di UE) yang memproses data pribadi subjek data UE sehubungan dengan penawaran barang atau jasa kepada subjek data di UE atau pemantauan perilaku yang terjadi di UE. Data pribadi adalah informasi apa pun yang berhubungan dengan orang alami yang teridentifikasi atau dapat diidentifikasi.

Anda dapat menemukan kerangka kerja GDPR di halaman pustaka kerangka Audit Manager. Untuk informasi selengkapnya, lihat [Pusat Peraturan Perlindungan Data Umum \(GDPR\)](#).

Menggunakan Framework ini

Anda dapat menggunakan kerangka kerja GDPR 2016 di Audit Manager untuk membantu Anda mempersiapkan audit.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Peraturan Perlindungan Data Umum (GDPR) 2016	0	378	10

Kerangka standar ini hanya berisi kontrol manual.

Note

Jika ingin mengotomatiskan pengumpulan bukti untuk GDPR, Anda dapat menggunakan Audit Manager untuk [membuat kontrol kustom Anda sendiri](#) untuk GDPR. Tabel berikut memberikan rekomendasi tentang sumber AWS data yang dapat Anda petakan ke persyaratan GDPR dalam kontrol kustom Anda. Meskipun beberapa sumber data berikut dipetakan ke beberapa kontrol, perlu diingat bahwa Anda hanya dikenakan biaya sekali untuk setiap penilaian sumber daya.

Rekomendasi berikut digunakan AWS Config dan AWS Security Hub CSPM sebagai sumber data. Agar berhasil mengumpulkan bukti dari sumber data ini, pastikan bahwa Anda mengikuti instruksi untuk [mengaktifkan dan mengatur AWS Config dan AWS Security Hub CSPM](#) di dalam Akun AWS. Setelah menyiapkan kedua layanan dengan cara ini, Audit Manager mengumpulkan bukti setiap kali evaluasi dilakukan untuk AWS Config aturan yang ditentukan atau kontrol CSPM Security Hub.

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 25 Perlindungan data berdasarkan desain dan secara default.1	Bab 4 - Pengontrol dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: - Tampilkan semua peristiwa akun root selama jangka waktu - AWS CloudTrail ember tidak publik

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• Tampilkan semua kebijakan dengan <code>Allow:*:*</code> dan cantumkan semua prinsipal dan layanan menggunakan kebijakan tersebut Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_DIPUTAR • IAM_PASSWORD_POLICY Pilih AWS Security Hub CSPM sebagai tipe sumber data, dan pilih kontrol Security Hub berikut sebagai pemetaan sumber data: • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5) • 1.20 (IAM.18) • 1.22 (IAM.1) • 1.3 (IAM.8)

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Konfigurasi.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Konfigurasi.1

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 25 Perlindungan data berdasarkan desain dan secara default.2	Bab 4 - Pengontrol dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan semua peristiwa akun root selama jangka waktu • AWS CloudTrail ember tidak publik • Tampilkan semua kebijakan dengan Allow:*:* dan cantumkan semua prinsipal dan layanan menggunakan kebijakan tersebut Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_DIPUTAR • IAM_PASSWORD_POLICY Pilih AWS Security Hub CSPM sebagai tipe sumber data, dan pilih kontrol Security Hub berikut sebagai pemetaan sumber data: • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4)

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5) • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Konfigurasi.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14)

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• Konfigurasi.1

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 25 Perlindungan data berdasarkan desain dan secara default.3	Bab 4 - Pengontrol dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan semua peristiwa akun root selama jangka waktu • AWS CloudTrail ember tidak publik • Tampilkan semua kebijakan dengan Allow:*:* dan cantumkan semua prinsipal dan layanan menggunakan kebijakan tersebut Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_DIPUTAR • IAM_PASSWORD_POLICY Pilih AWS Security Hub CSPM sebagai tipe sumber data, dan pilih kontrol Security Hub berikut sebagai pemetaan sumber data: • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4)

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5) • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Konfigurasi.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14)

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• Konfigurasi.1
Pasal 30 Catatan kegiatan pemrosesan.1	Bab 4 - Pengontrolan dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan semua peristiwa akun root selama jangka waktu Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUDTRAIL_SECURITY_TRAIL_ENABLED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Pilih AWS Security Hub CSPM sebagai tipe sumber data, dan pilih kontrol Security Hub berikut sebagai pemetaan sumber data: • Konfigurasi.1

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 30 Catatan kegiatan pemrosesan.2	Bab 4 - Pengontrolan dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan semua peristiwa akun root selama jangka waktu Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Pilih AWS Security Hub CSPM sebagai tipe sumber data, dan pilih kontrol Security Hub berikut sebagai pemetaan sumber data: • Konfigurasi.1

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 30 Catatan kegiatan pemrosesan.3	Bab 4 - Pengontrolan dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan semua peristiwa akun root selama jangka waktu • AWS CloudTrail ember tidak publik • Tampilkan semua kebijakan dengan Allow: * : * dan cantumkan semua prinsipal dan layanan menggunakan kebijakan tersebut Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Pilih AWS Security Hub CSPM sebagai tipe sumber data, dan pilih kontrol Security Hub berikut sebagai pemetaan sumber data: • Konfigurasi.1

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 30 Catatan kegiatan pemrosesan.4	Bab 4 - Pengontrol I dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan semua peristiwa akun root selama jangka waktu • AWS CloudTrail ember tidak publik • Tampilkan semua kebijakan dengan Allow: * : * dan cantumkan semua prinsipal dan layanan menggunakan kebijakan tersebut Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Pilih AWS Security Hub CSPM sebagai tipe sumber data, dan pilih kontrol Security Hub berikut sebagai pemetaan sumber data: • Konfigurasi.1

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 30 Catatan kegiatan pemrosesan.5	Bab 4 - Pengontrolan dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan semua peristiwa akun root selama jangka waktu Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Pilih AWS Security Hub CSPM sebagai tipe sumber data, dan pilih kontrol Security Hub berikut sebagai pemetaan sumber data: • Konfigurasi.1

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 32 Keamanan pemrosesan.1	Bab 4 - Pengontrol dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan enkripsi data saat istirahat untuk semua layanan • Tampilkan data dalam enkripsi transit untuk semua layanan • MFA Hapus diaktifkan untuk Amazon S3 • Semua pemindaian Amazon Inspector • Tampilkan semua instans yang tidak diaktifkan Amazon Inspector • Tampilkan semua penyeimbang beban yang mendengarkan di HTTPS (SSL) • AWS CloudTrail dienkripsi saat istirahat • Amazon CloudWatch memberi peringatan untuk AWS Config menampilkan semua perubahan dan semua pengaturan yang dikomentari • Semua aktivitas root Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • TERENKRIPTEKED_VOLUME

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• <u>RDS_STORAGE_TERENKRIPSI</u> • <u>REDSHIFT_CLUSTER_CONFIGURATION_CHECK</u> • <u>S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED</u> • <u>SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURATED</u> • <u>SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURATED</u> • <u>SNS_ENCRYPTED_KMS</u> • <u>EC2_EBS_ENCRYPTION_BY_DEFAULT</u> • <u>DYNAMODB_TABLE_ENCRYPTED_KMS</u> • <u>DYNAMODB_TABLE_ENCRYPTION_ENABLED</u> • <u>RDS_SNAPSHOT_ENCRYPTED</u> • <u>S3_DEFAULT_ENCRYPTION_KMS</u> • <u>DAX_ENCRYPTION_ENABLED</u> • <u>EKS_SECRETS_ENCRYPTED</u> • <u>RDS_LOGGING_ENABLED</u> • <u>REDSHIFT_BACKUP_ENABLED</u> • <u>RDS_IN_BACKUP_PLAN</u> • <u>WAF_CLASSIC_LOGGING_ENABLED</u> • <u>WAFV2_LOGGING_ENABLED</u> • <u>ALB_HTTP_TO_HTTP_REDIRECTION_CHECK</u> • <u>ELB_ACM_CERTIFICATE_REQUIRED</u> • <u>ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK</u> • <u>REDSHIFT_REQUIRE_TLS_SSL</u> • <u>CLOUDFRONT_VIEWER_POLICY_HTTPS</u> • <u>ALB_HTTP_DROP_INVALID_HEADER_ENABLED</u> • <u>ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK</u> • <u>ELB_TLS_HTTPS_LISTENERS_ONLY</u> • <u>ACM_CERTIFICATE_EXPIRATION_CHECK</u>

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• <u>API_GW_CACHE_ENABLED_AND_TERENKRIPSI</u>

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 32 Keamanan pemrosesan.2	Bab 4 - Pengontrolan dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan enkripsi data saat istirahat untuk semua layanan • Tampilkan data dalam enkripsi transit untuk semua layanan • MFA Hapus diaktifkan untuk Amazon S3 • Semua pemindaian Amazon Inspector • Tampilkan semua instans yang tidak diaktifkan Amazon Inspector • Tampilkan semua penyeimbang beban yang mendengarkan di HTTPS (SSL) • AWS CloudTrail dienkripsi saat istirahat • Amazon CloudWatch memberi peringatan untuk AWS Config menampilkan semua perubahan dan semua pengaturan yang dikomentari • Semua aktivitas root Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • TERENKRIPTED_VOLUME

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• <u>RDS_STORAGE_TERENKRIPSI</u> • <u>REDSHIFT_CLUSTER_CONFIGURATION_CHECK</u> • <u>S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED</u> • <u>SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURATED</u> • <u>SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURATED</u> • <u>SNS_ENCRYPTED_KMS</u> • <u>EC2_EBS_ENCRYPTION_BY_DEFAULT</u> • <u>DYNAMODB_TABLE_ENCRYPTED_KMS</u> • <u>DYNAMODB_TABLE_ENCRYPTION_ENABLED</u> • <u>RDS_SNAPSHOT_ENCRYPTED</u> • <u>S3_DEFAULT_ENCRYPTION_KMS</u> • <u>DAX_ENCRYPTION_ENABLED</u> • <u>EKS_SECRETS_ENCRYPTED</u> • <u>RDS_LOGGING_ENABLED</u> • <u>REDSHIFT_BACKUP_ENABLED</u> • <u>RDS_IN_BACKUP_PLAN</u> • <u>WAF_CLASSIC_LOGGING_ENABLED</u> • <u>WAFV2_LOGGING_ENABLED</u> • <u>ALB_HTTP_TO_HTTP_REDIRECTION_CHECK</u> • <u>ELB_ACM_CERTIFICATE_REQUIRED</u> • <u>ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK</u> • <u>REDSHIFT_REQUIRE_TLS_SSL</u> • <u>CLOUDFRONT_VIEWER_POLICY_HTTPS</u> • <u>ALB_HTTP_DROP_INVALID_HEADER_ENABLED</u> • <u>ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK</u> • <u>ELB_TLS_HTTPS_LISTENERS_ONLY</u> • <u>ACM_CERTIFICATE_EXPIRATION_CHECK</u>

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• API_GW_CACHE_ENABLED_AND_TERENKRIPSI

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 32 Keamanan pemrosesan.3	Bab 4 - Pengontrol dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan enkripsi data saat istirahat untuk semua layanan • Tampilkan data dalam enkripsi transit untuk semua layanan • MFA Hapus diaktifkan untuk Amazon S3 • Semua pemindaian Amazon Inspector • Tampilkan semua instans yang tidak diaktifkan Amazon Inspector • Tampilkan semua penyeimbang beban yang mendengarkan di HTTPS (SSL) • AWS CloudTrail dienkripsi saat istirahat • Amazon CloudWatch memberi peringatan untuk AWS Config menampilkan semua perubahan dan semua pengaturan yang dikomentari • Semua aktivitas root Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • TERENKRIPTED_VOLUME

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• <u>RDS_STORAGE_TERENKRIPSI</u> • <u>REDSHIFT_CLUSTER_CONFIGURATION_CHECK</u> • <u>S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED</u> • <u>SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURATED</u> • <u>SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURATED</u> • <u>SNS_ENCRYPTED_KMS</u> • <u>EC2_EBS_ENCRYPTION_BY_DEFAULT</u> • <u>DYNAMODB_TABLE_ENCRYPTED_KMS</u> • <u>DYNAMODB_TABLE_ENCRYPTION_ENABLED</u> • <u>RDS_SNAPSHOT_ENCRYPTED</u> • <u>S3_DEFAULT_ENCRYPTION_KMS</u> • <u>DAX_ENCRYPTION_ENABLED</u> • <u>EKS_SECRETS_ENCRYPTED</u> • <u>RDS_LOGGING_ENABLED</u> • <u>REDSHIFT_BACKUP_ENABLED</u> • <u>RDS_IN_BACKUP_PLAN</u> • <u>WAF_CLASSIC_LOGGING_ENABLED</u> • <u>WAFV2_LOGGING_ENABLED</u> • <u>ALB_HTTP_TO_HTTP_REDIRECTION_CHECK</u> • <u>ELB_ACM_CERTIFICATE_REQUIRED</u> • <u>ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK</u> • <u>REDSHIFT_REQUIRE_TLS_SSL</u> • <u>CLOUDFRONT_VIEWER_POLICY_HTTPS</u> • <u>ALB_HTTP_DROP_INVALID_HEADER_ENABLED</u> • <u>ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK</u> • <u>ELB_TLS_HTTPS_LISTENERS_ONLY</u> • <u>ACM_CERTIFICATE_EXPIRATION_CHECK</u>

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• <u>API_GW_CACHE_ENABLED_AND_TERENKRIPSI</u>

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
Pasal 32 Keamanan pemrosesan.4	Bab 4 - Pengontrolan dan Prosesor	Anda dapat membuat kontrol khusus AWS Audit Manager yang mendukung kontrol GDPR ini. Saat Anda menentukan detail kontrol, masukkan yang berikut ini di bawah Informasi pengujian: • Tampilkan enkripsi data saat istirahat untuk semua layanan • Tampilkan data dalam enkripsi transit untuk semua layanan • MFA Hapus diaktifkan untuk Amazon S3 • Semua pemindaian Amazon Inspector • Tampilkan semua instans yang tidak diaktifkan Amazon Inspector • Tampilkan semua penyeimbang beban yang mendengarkan di HTTPS (SSL) • AWS CloudTrail dienkripsi saat istirahat • Amazon CloudWatch memberi peringatan untuk AWS Config menampilkan semua perubahan dan semua pengaturan yang dikomentari • Semua aktivitas root Saat Anda mengatur sumber data kontrol, sebaiknya sertakan semua hal berikut sebagai sumber data: Pilih AWS Config sebagai tipe sumber data, dan pilih aturan AWS Config terkelola berikut sebagai pemetaan sumber data: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • TERENKRIPTED_VOLUME

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• <u>RDS_STORAGE_TERENKRIPSI</u> • <u>REDSHIFT_CLUSTER_CONFIGURATION_CHECK</u> • <u>S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED</u> • <u>SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURATED</u> • <u>SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURATED</u> • <u>SNS_ENCRYPTED_KMS</u> • <u>EC2_EBS_ENCRYPTION_BY_DEFAULT</u> • <u>DYNAMODB_TABLE_ENCRYPTED_KMS</u> • <u>DYNAMODB_TABLE_ENCRYPTION_ENABLED</u> • <u>RDS_SNAPSHOT_ENCRYPTED</u> • <u>S3_DEFAULT_ENCRYPTION_KMS</u> • <u>DAX_ENCRYPTION_ENABLED</u> • <u>EKS_SECRETS_ENCRYPTED</u> • <u>RDS_LOGGING_ENABLED</u> • <u>REDSHIFT_BACKUP_ENABLED</u> • <u>RDS_IN_BACKUP_PLAN</u> • <u>WAF_CLASSIC_LOGGING_ENABLED</u> • <u>WAFV2_LOGGING_ENABLED</u> • <u>ALB_HTTP_TO_HTTP_REDIRECTION_CHECK</u> • <u>ELB_ACM_CERTIFICATE_REQUIRED</u> • <u>ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK</u> • <u>REDSHIFT_REQUIRE_TLS_SSL</u> • <u>CLOUDFRONT_VIEWER_POLICY_HTTPS</u> • <u>ALB_HTTP_DROP_INVALID_HEADER_ENABLED</u> • <u>ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK</u> • <u>ELB_TLS_HTTPS_LISTENERS_ONLY</u> • <u>ACM_CERTIFICATE_EXPIRATION_CHECK</u>

Nama kontrol	Set kontrol	Pemetaan sumber data kontrol yang disarankan
		• API_GW_CACHE_ENABLED_AND_TERENKRIPSI

Setelah Anda membuat kontrol kustom baru untuk GDPR, Anda dapat menambahkannya ke kerangka kerja GDPR kustom. Anda kemudian dapat membuat penilaian dari kerangka kerja GDPR khusus. Dengan cara ini, Audit Manager dapat mengumpulkan bukti secara otomatis untuk kontrol kustom yang Anda tambahkan.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [Pusat Peraturan Perlindungan Data Umum \(GDPR\)](#)
- [AWS Postingan blog GDPR](#)

Gramm-Leach-Bliley Bertindak

AWS Audit Manager menyediakan kerangka kerja prebuilt yang mendukung Gramm-Leach-Bliley Undang-Undang (GLBA).

Topik

- [Apa itu GLBA?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)

Apa itu GLBA?

GLBA (atau Undang-Undang GLB), juga dikenal sebagai Undang-Undang Modernisasi Layanan Keuangan tahun 1999, adalah undang-undang federal yang diberlakukan di Amerika Serikat untuk mengontrol cara-cara lembaga keuangan menangani informasi pribadi individu. Undang-undang ini terdiri dari tiga bagian. Yang pertama adalah Aturan Privasi Keuangan, yang mengatur pengumpulan dan pengungkapan informasi keuangan pribadi. Yang kedua adalah Aturan Pengamanan, yang menetapkan bahwa lembaga keuangan harus menerapkan program keamanan untuk melindungi informasi tersebut. Yang ketiga adalah ketentuan Pretexting, yang melarang praktik pretexting (mengakses informasi pribadi menggunakan kepura-puraan palsu). Undang-undang ini juga mewajibkan lembaga keuangan untuk memberikan pemberitahuan privasi tertulis kepada pelanggan yang menjelaskan praktik berbagi informasi mereka.

Menggunakan Framework ini

Anda dapat menggunakan kerangka kerja GLBA 2016 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan GLBA. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja GLBA sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit GLBA. Dalam penilaian Anda, Anda dapat menentukan Akun AWS yang ingin Anda sertakan dalam lingkup audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka GLBA. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Gramm-Leach-Bliley Bertindak (GLBA)	0	120	16

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan standar GLBA. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit GLBA. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Judul 21 CFR Bagian 11

AWS Audit Manager menyediakan kerangka standar bawaan yang mendukung Judul 21 dari Kode Peraturan Federal (CFR) Bagian 11, Catatan elektronik; Tanda Tangan Elektronik - Lingkup dan Aplikasi 24 Mei 2023.

Topik

- [Apa Judul 21 dari CFR Bagian 11?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa Judul 21 dari CFR Bagian 11?

GxP mengacu pada peraturan dan pedoman yang berlaku untuk organisasi ilmu hayati yang membuat makanan dan produk medis. Produk medis yang termasuk dalam ini termasuk obat-obatan, perangkat medis, dan aplikasi perangkat lunak medis. Tujuan keseluruhan dari persyaratan GxP adalah untuk memastikan bahwa makanan dan produk medis aman bagi konsumen. Ini juga untuk memastikan integritas data yang digunakan untuk membuat keputusan keselamatan terkait produk.

Di Amerika Serikat, peraturan GxP diberlakukan oleh Food and Drug Administration (FDA) AS, dan tercantum dalam Judul 21 dari Kode Peraturan Federal (21 CFR). Dalam 21 CFR, Bagian 11 berisi persyaratan untuk sistem komputer yang membuat, memodifikasi, memelihara, mengarsipkan, mengambil, atau mendistribusikan catatan elektronik dan tanda tangan elektronik untuk mendukung kegiatan yang diatur GXP. Bagian 11 dibuat untuk memungkinkan adopsi teknologi informasi baru oleh organisasi ilmu hayati yang diatur FDA, sekaligus menyediakan kerangka kerja untuk memastikan bahwa data GxP elektronik dapat dipercaya dan dapat diandalkan.

Untuk pendekatan komprehensif dalam menggunakan AWS Cloud untuk sistem GxP, lihat whitepaper [Pertimbangan untuk Menggunakan AWS Produk di Sistem GxP](#).

Menggunakan Framework ini

Anda dapat menggunakan kerangka kerja Judul 21 CFR Bagian 11 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan CFR. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka Judul 21 CFR Bagian 11. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Judul 21 Kode Peraturan Federal (CFR) Bagian 11, Catatan elektronik; Tanda Tangan Elektronik - Lingkup dan Aplikasi 24 Mei 2023	6	19	2

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM. Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file [AuditManager_ConfigDataSourceMappings_Title-21-CFR-Part-11.zip](#).

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan peraturan GxP. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [AWS Halaman kepatuhan untuk GxP](#)

- [Pertimbangan untuk Menggunakan AWS Produk dalam Sistem GxP](#)

Lampiran GMP UE 11, v1

AWS Audit Manager menyediakan kerangka kerja bawaan yang mendukung EudraLex - Aturan yang Mengatur Produk Obat di Uni Eropa (UE) - Volume 4: Good Manufacturing Practice (GMP) Produk Obat untuk Penggunaan Manusia dan Hewan - Lampiran 11.

Topik

- [Apa itu EU GMP Annex 11?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)

Apa itu EU GMP Annex 11?

Kerangka kerja EU GMP Annex 11 adalah setara Eropa dengan kerangka kerja Judul 21 CFR bagian 11 di Amerika Serikat. Lampiran ini berlaku untuk semua bentuk sistem komputerisasi yang digunakan sebagai bagian dari kegiatan yang diatur Good Manufacturing Practices (GMP). Sistem komputerisasi adalah seperangkat komponen perangkat lunak dan perangkat keras yang bersama-sama memenuhi fungsionalitas tertentu. Aplikasi harus divalidasi dan infrastruktur TI harus memenuhi syarat. Jika sistem komputerisasi menggantikan operasi manual, seharusnya tidak ada penurunan kualitas produk, kontrol proses, atau jaminan kualitas yang dihasilkan. Seharusnya tidak ada peningkatan risiko keseluruhan dari proses tersebut.

Lampiran 11 adalah bagian dari pedoman GMP Eropa dan mendefinisikan kerangka acuan untuk sistem komputerisasi yang digunakan oleh organisasi di industri farmasi. Lampiran 11 berfungsi sebagai daftar Periksa yang memungkinkan badan pengatur Eropa untuk menetapkan persyaratan untuk sistem komputerisasi yang berhubungan dengan produk farmasi dan perangkat medis. Pedoman yang ditetapkan oleh Komisi Komite Eropa tidak jauh dari FDA (Judul 21 CFR Bagian 11). Lampiran 11 mendefinisikan kriteria bagaimana catatan elektronik dan tanda tangan elektronik dianggap dikelola.

Menggunakan Framework ini

Anda dapat menggunakan kerangka kerja EU GMP Annex 11 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi

dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan GMP UE. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka kerja EU GMP Annex 11. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
EudraLex - Aturan yang Mengatur Produk Obat di Uni Eropa (UE) - Volume 4: Good Manufacturing Practice (GMP) Produk Obat untuk Penggunaan Manusia dan Hewan - Lampiran 11	0	32	3

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file [AuditManager_ConfigDataSourceMappings_EudraLex-GMP-Volume-4-Annex-11.zip](#).

Kontrol dalam kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan persyaratan EU GMP Annex 11. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit GMP UE. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Aturan Keamanan HIPAA: Feb 2003

AWS Audit Manager menyediakan kerangka standar bawaan yang mendukung Aturan Keamanan Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA): Feb 2003.

Note

Untuk informasi tentang HIPAA Final Omnibus Security Rule 2013 dan framework Audit Manager yang mendukung standar ini, lihat. [Aturan Akhir Omnibus HIPAA](#)

Topik

- [Apa itu HIPAA dan Aturan Keamanan HIPAA 2003?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu HIPAA dan Aturan Keamanan HIPAA 2003?

HIPAA adalah undang-undang yang membantu pekerja AS untuk mempertahankan cakupan asuransi kesehatan ketika mereka berganti atau kehilangan pekerjaan. Undang-undang ini juga

berupaya mendorong catatan kesehatan elektronik untuk meningkatkan efisiensi dan kualitas sistem perawatan kesehatan AS melalui peningkatan berbagi informasi.

Seiring dengan meningkatnya penggunaan catatan medis elektronik, HIPAA mencakup ketentuan untuk melindungi keamanan dan privasi informasi kesehatan yang dilindungi (PHI). PHI mencakup serangkaian data kesehatan dan kesehatan yang dapat diidentifikasi secara pribadi yang sangat luas. Ini termasuk informasi asuransi dan penagihan, data diagnosis, data perawatan klinis, dan hasil lab seperti gambar dan hasil tes.

Departemen Kesehatan dan Layanan Kemanusiaan AS menerbitkan [Aturan Keamanan](#) final pada Februari 2003. Aturan ini menetapkan standar nasional untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi kesehatan yang dilindungi secara elektronik.

Aturan HIPAA berlaku untuk entitas yang dilindungi. Ini termasuk rumah sakit, penyedia layanan medis, rencana kesehatan yang disponsori majikan, fasilitas penelitian, dan perusahaan asuransi yang berurusan langsung dengan pasien dan data pasien. Persyaratan HIPAA untuk melindungi PHI juga meluas ke rekan bisnis.

Untuk informasi selengkapnya tentang bagaimana HIPAA dan HITECH melindungi informasi [kesehatan, lihat halaman web Privasi Informasi Kesehatan](#) dari Departemen Kesehatan dan Layanan Kemanusiaan AS.

Semakin banyak penyedia layanan kesehatan, pembayar, dan profesional TI menggunakan layanan cloud AWS berbasis utilitas untuk memproses, menyimpan, dan mengirimkan informasi kesehatan yang dilindungi (PHI). AWS memungkinkan entitas yang dilindungi dan rekan bisnis mereka yang tunduk pada HIPAA untuk menggunakan AWS lingkungan yang aman untuk memproses, memelihara, dan menyimpan informasi kesehatan yang dilindungi.

Untuk petunjuk tentang cara Anda dapat menggunakan AWS untuk pemrosesan dan penyimpanan informasi kesehatan, lihat whitepaper [Architecting for HIPAA Security and Compliance on Amazon Web Services](#).

Menggunakan Framework ini

Anda dapat menggunakan kerangka HIPAA Security Rule 2003 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan HIPAA. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka HIPAA. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Aturan Keamanan Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA): Feb 2003	24	61	5

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM. Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file [AuditManager_ConfigDataSourceMappings_HIPAA-Security-Rule-Feb-2003.zip](#).

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan standar HIPAA. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit HIPAA. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [Informasi Kesehatan Privasi](#) dari Departemen Kesehatan dan Layanan Kemanusiaan AS
- [Aturan Keamanan](#) dari Departemen Kesehatan dan Layanan Kemanusiaan AS
- [Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services](#)
- [AWS Halaman kepatuhan untuk HIPAA](#)

Aturan Akhir Omnibus HIPAA

AWS Audit Manager menyediakan kerangka standar bawaan yang mendukung Aturan Akhir Omnibus Omnibus Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA).

Note

Untuk informasi tentang Aturan Keamanan HIPAA 2003 dan AWS Audit Manager kerangka kerja yang mendukung standar ini, lihat [Aturan Keamanan HIPAA: Feb 2003](#).

Topik

- [Apa itu HIPAA dan Aturan Keamanan Omnibus Akhir HIPAA?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu HIPAA dan Aturan Keamanan Omnibus Akhir HIPAA?

HIPAA adalah undang-undang yang membantu pekerja AS untuk mempertahankan cakupan asuransi kesehatan ketika mereka berganti atau kehilangan pekerjaan. Undang-undang ini juga berupaya mendorong catatan kesehatan elektronik untuk meningkatkan efisiensi dan kualitas sistem perawatan kesehatan AS melalui peningkatan berbagi informasi.

Seiring dengan meningkatnya penggunaan catatan medis elektronik, HIPAA mencakup ketentuan untuk melindungi keamanan dan privasi informasi kesehatan yang dilindungi (PHI). PHI mencakup serangkaian data kesehatan dan kesehatan yang dapat diidentifikasi secara pribadi yang sangat luas. Ini termasuk informasi asuransi dan penagihan, data diagnosis, data perawatan klinis, dan hasil lab seperti gambar dan hasil tes.

Aturan Keamanan Omnibus Final HIPAA, yang menjadi efektif pada tahun 2013, menerapkan sejumlah pembaruan untuk semua aturan yang disahkan sebelumnya. Modifikasi pada Keamanan, Privasi, Pemberitahuan Pelanggaran, dan Aturan Penegakan dimaksudkan untuk meningkatkan kerahasiaan dan keamanan dalam berbagi data.

Aturan HIPAA berlaku untuk entitas yang dilindungi. Ini termasuk rumah sakit, penyedia layanan medis, rencana kesehatan yang disponsori majikan, fasilitas penelitian, dan perusahaan asuransi yang berurusan langsung dengan pasien dan data pasien. Sebagai bagian dari pembaruan omnibus, banyak aturan HIPAA yang berlaku untuk entitas yang tercakup juga sekarang berlaku untuk rekan bisnis.

Untuk informasi selengkapnya tentang bagaimana HIPAA dan HITECH melindungi informasi [kesehatan, lihat halaman web Privasi Informasi Kesehatan](#) dari Departemen Kesehatan dan Layanan Kemanusiaan AS.

Semakin banyak penyedia layanan kesehatan, pembayar, dan profesional TI menggunakan layanan cloud AWS berbasis utilitas untuk memproses, menyimpan, dan mengirimkan informasi kesehatan yang dilindungi (PHI). AWS memungkinkan entitas yang dilindungi dan rekan bisnis mereka yang tunduk pada HIPAA untuk menggunakan AWS lingkungan yang aman untuk memproses, memelihara, dan menyimpan informasi kesehatan yang dilindungi. Untuk petunjuk tentang cara Anda dapat menggunakan AWS untuk pemrosesan dan penyimpanan informasi kesehatan, lihat whitepaper [Architecting for HIPAA Security and Compliance on Amazon Web Services](#).

Menggunakan Framework ini

Anda dapat menggunakan kerangka HIPAA Omnibus Final Rule untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi

dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan HIPAA. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka HIPAA. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Aturan Akhir Omnibus Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA)	21	53	5

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM. Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file [AuditManager_ConfigDataSourceMappings_HIPAA-Omnibus-Final-Rule.zip](#).

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan standar HIPAA. Selain itu, mereka tidak dapat menjamin bahwa Anda

akan lulus audit HIPAA. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [Informasi Kesehatan Privasi](#) dari Departemen Kesehatan dan Layanan Kemanusiaan AS
- [Omnibus HIPAA Rulemaking](#) dari Departemen Kesehatan dan Layanan Kemanusiaan AS
- [Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services](#)
- [AWS Halaman kepatuhan untuk HIPAA](#)

ISO/IEC 27001:2013 Lampiran A

AWS Audit Manager menyediakan kerangka standar bawaan yang mendukung Organisasi Internasional untuk standardisasi (ISO) /Komisi Elektroteknik Internasional (IEC) 27001:2013 Lampiran A.

Topik

- [Apa itu ISO/IEC 27001:2013 Lampiran A?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu ISO/IEC 27001:2013 Lampiran A?

Komisi Elektroteknik Internasional (IEC) dan Organisasi Internasional untuk Standardisasi (ISO) keduanya independen, non-pemerintah, not-for-profit organisasi yang mengembangkan dan menerbitkan standar internasional berbasis konsensus sepenuhnya.

ISO/IEC 27001:2013 Annex A is a security management standard that specifies security management best practices and comprehensive security controls that follow the ISO/IEC27002 bimbingan praktik terbaik. Standar internasional ini menetapkan persyaratan tentang bagaimana membangun, menerapkan, memelihara, dan terus meningkatkan sistem manajemen keamanan informasi di organisasi Anda. Termasuk di antara standar-standar ini adalah persyaratan pada penilaian dan perlakuan risiko keamanan informasi yang disesuaikan dengan kebutuhan organisasi Anda. Persyaratan dalam standar internasional ini bersifat generik dan dimaksudkan untuk berlaku untuk semua organisasi, terlepas dari jenis, ukuran atau sifatnya.

Menggunakan Framework ini

Anda dapat menggunakan AWS Audit Manager kerangka kerja untuk ISO/IEC 27001:2013 Lampiran A untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan ISO/IEC 27001:2013 Lampiran A. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Lampiran A ISO/IEC 27001:2013. Dalam penilaian Anda, Anda dapat menentukan Akun AWS yang ingin Anda sertakan dalam lingkup audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam ISO/IEC 27001:2013 Annex A framework. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksponnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Organisasi Internasional untuk Standardisasi (ISO) / Komisi Elektroteknik Internasional (IEC) 27001:2013 Lampiran A	21	93	35

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM. Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file [AuditManager_ConfigDataSourceMappings_ISO-IEC-270012013-Annex-A.zip](#).

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan standar internasional ini. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus ISO/IEC audit. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- Untuk informasi lebih lanjut tentang standar internasional ini, lihat [ISO/IEC 27001: 2013](#) di ANSI Webstore.

NIST SP 800-53 Rev 5

AWS Audit Manager menyediakan kerangka kerja bawaan yang mendukung NIST 800-53 Rev 5: Security and Privacy Controls for Information Systems and Organizations.

Note

- Untuk informasi tentang kerangka Audit Manager yang mendukung NIST SP 800-171, lihat. [NIST SP 800-171 Rev 2](#)
- Untuk informasi tentang framework Audit Manager yang mendukung NIST CSF, lihat. [Kerangka Keamanan Siber NIST v1.1](#)

Topik

- [Apa itu NIST SP 800-53?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu NIST SP 800-53?

[National Institute of Standards and Technology \(NIST\)](#) didirikan pada tahun 1901 dan sekarang menjadi bagian dari Departemen Perdagangan AS. NIST adalah salah satu laboratorium ilmu fisika tertua di Amerika Serikat. Kongres AS membentuk badan tersebut untuk memperbaiki apa yang pada saat itu merupakan infrastruktur pengukuran kelas dua. Infrastruktur merupakan tantangan besar bagi daya saing industri AS, setelah tertinggal dari kekuatan ekonomi lainnya seperti Inggris dan Jerman.

Kontrol keamanan NIST SP 800-53 umumnya berlaku untuk sistem informasi federal AS. Ini biasanya sistem yang harus melalui penilaian formal dan proses otorisasi. Proses ini memastikan perlindungan

yang memadai atas kerahasiaan, integritas, dan ketersediaan sistem informasi dan informasi. Ini didasarkan pada kategori keamanan dan tingkat dampak sistem (rendah, sedang, atau tinggi) serta penentuan risiko. Kontrol keamanan dipilih dari katalog kontrol keamanan NIST SP 800-53, dan sistem dinilai terhadap persyaratan kontrol keamanan tersebut.

Kerangka kerja NIST SP 800-53 mewakili kontrol keamanan dan prosedur penilaian terkait yang didefinisikan dalam NIST SP 800-53 Revisi 5 Kontrol Keamanan yang Direkomendasikan untuk Sistem dan Organisasi Informasi Federal. [Untuk setiap perbedaan yang dicatat dalam konten antara kerangka kerja NIST SP 800-53 ini dan Publikasi Khusus NIST yang diterbitkan terbaru SP 800-53 Revisi 5, lihat dokumen resmi yang diterbitkan yang tersedia di Pusat Sumber Daya Keamanan Komputer NIST.](#)

Menggunakan Framework ini

Anda dapat menggunakan kerangka kerja NIST SP 800-53 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan NIST. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka kerja NIST SP 800-53. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
NIST 800-53 Rev 5: Kontrol Keamanan dan Privasi	132	875	20

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
untuk Sistem Informasi dan Organizations			

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM. Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file [AuditManager_ConfigDataSourceMappings_NIST-800-53-Rev-5.zip](#).

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan standar NIST. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit NIST. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [Institut Nasional Standar dan Teknologi \(NIST\)](#)
- [Pusat Sumber Daya Keamanan Komputer NIST](#)
- [AWS Halaman kepatuhan untuk NIST](#)

Kerangka Keamanan Siber NIST v1.1

AWS Audit Manager menyediakan kerangka kerja bawaan yang mendukung NIST Cybersecurity Framework (CSF) v1.1.

Note

- Untuk informasi tentang kerangka Audit Manager yang mendukung NIST SP 800-53, lihat. [NIST SP 800-53 Rev 5](#)
- Untuk informasi tentang kerangka Audit Manager yang mendukung NIST SP 800-171, lihat. [NIST SP 800-171 Rev 2](#)

Topik

- [Apa itu Kerangka Keamanan Siber NIST?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu Kerangka Keamanan Siber NIST?

[National Institute of Standards and Technology \(NIST\)](#) didirikan pada tahun 1901 dan sekarang menjadi bagian dari Departemen Perdagangan AS. NIST adalah salah satu laboratorium ilmu fisika tertua di Amerika Serikat. Kongres AS membentuk badan tersebut untuk memperbaiki apa yang pada saat itu merupakan infrastruktur pengukuran kelas dua. Infrastruktur merupakan tantangan besar bagi daya saing industri AS, setelah tertinggal dari kekuatan ekonomi lainnya seperti Inggris dan Jerman.

Amerika Serikat bergantung pada fungsi infrastruktur kritis yang andal. Ancaman keamanan siber mengeksplotasi peningkatan kompleksitas dan keterkaitan sistem infrastruktur kritis. Mereka menempatkan keamanan, ekonomi, dan keselamatan publik dan kesehatan Amerika Serikat dalam bahaya. Mirip dengan risiko keuangan dan reputasi, risiko keamanan siber memengaruhi laba perusahaan. Hal ini dapat meningkatkan biaya dan mempengaruhi pendapatan. Hal ini dapat membahayakan kemampuan organisasi untuk berinovasi dan untuk mendapatkan dan mempertahankan pelanggan. Pada akhirnya, keamanan siber dapat memperkuat manajemen risiko keseluruhan organisasi.

NIST Cybersecurity Framework (CSF) didukung oleh pemerintah dan industri di seluruh dunia sebagai dasar yang direkomendasikan untuk digunakan oleh organisasi mana pun, terlepas dari sektor atau ukurannya. Kerangka Keamanan Siber NIST terdiri dari tiga komponen utama: inti kerangka kerja, profil, dan tingkatan implementasi. Inti kerangka kerja berisi aktivitas dan hasil keamanan siber yang diinginkan yang diatur dalam 23 kategori yang mencakup luasnya tujuan keamanan siber untuk suatu organisasi. Profil berisi keselarasan unik organisasi dari persyaratan dan tujuan organisasi mereka, selera risiko, dan sumber daya menggunakan hasil yang diinginkan dari inti kerangka kerja. Tingkatan implementasi menggambarkan sejauh mana praktik manajemen risiko keamanan siber organisasi menunjukkan karakteristik yang didefinisikan dalam inti kerangka kerja.

Menggunakan Framework ini

Anda dapat menggunakan NIST CSF v1.1 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan CSF NIST. Audit Manager saat ini mendukung komponen inti kerangka kerja. Audit Manager tidak mendukung komponen profil dan implementasi dalam kerangka kerja ini.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Hal ini dilakukan berdasarkan kontrol yang didefinisikan dalam CSF NIST. Ketika tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Kerangka Keamanan Siber NIST (CSF) v1.1	14	94	22

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM. Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka kerja standar ini, unduh file [AuditManager_ ConfigDataSourceMappings _NIST-CSF-v1.1.zip](#).

Kontrol yang ditawarkan oleh Audit Manager tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan CSF NIST. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit NIST. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [Institut Nasional Standar dan Teknologi \(NIST\)](#)
- [Pusat Sumber Daya Keamanan Komputer NIST](#)
- [AWS Halaman kepatuhan untuk NIST](#)
- [Kerangka Keamanan Siber NIST - Menyelaraskan dengan NIST CSF di Cloud AWS](#)

NIST SP 800-171 Rev 2

AWS Audit Manager menyediakan kerangka kerja standar bawaan yang mendukung NIST 800-171 Revisi 2: Melindungi Informasi Tidak Terklasifikasi Terkendali dalam Sistem dan Organisasi Nonfederal.

 Note

- Untuk informasi tentang kerangka Audit Manager yang mendukung NIST SP 800-53, lihat. [NIST SP 800-53 Rev 5](#)
- Untuk informasi tentang framework Audit Manager yang mendukung NIST CSF, lihat. [Kerangka Keamanan Siber NIST v1.1](#)

Topik

- [Apa itu NIST SP 800-171?](#)
- [Menggunakan Framework ini](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu NIST SP 800-171?

NIST SP 800-171 berfokus pada melindungi kerahasiaan Controlled Unclassified Information (CUI) dalam sistem dan organisasi nonfederal. Ini merekomendasikan persyaratan keamanan khusus untuk mencapai tujuan itu. NIST 800-171 adalah publikasi yang menguraikan standar dan praktik keamanan yang diperlukan untuk organisasi nonfederal yang menangani CUI di jaringan mereka. Ini pertama kali diterbitkan pada Juni 2015 oleh [National Institute of Standards and Technology \(NIST\)](#). NIST adalah lembaga pemerintah AS yang merilis beberapa standar dan publikasi untuk memperkuat ketahanan keamanan siber di sektor publik dan swasta. NIST SP 800-171 telah menerima pembaruan rutin sejalan dengan ancaman dunia maya yang muncul dan teknologi yang berubah. Versi terbaru (revisi 2) dirilis pada Februari 2020.

Kontrol keamanan siber dalam NIST SP 800-171 melindungi CUI di jaringan TI kontraktor dan subkontraktor pemerintah. Ini mendefinisikan praktik dan prosedur yang harus dipatuhi oleh kontraktor pemerintah ketika jaringan mereka memproses atau menyimpan CUI. NIST SP 800-171 hanya berlaku untuk bagian-bagian jaringan kontraktor di mana CUI hadir.

Menggunakan Framework ini

Anda dapat menggunakan kerangka kerja NIST SP 800-171 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan NIST. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka kerja NIST SP 800-171. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
NIST 800-171 Revisi 2: Melindungi Informasi Tidak Diklasifikasikan Terkendali dalam Sistem dan Organisasi Nonfederal	35	75	14

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM. Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau

AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file [AuditManager_ConfigDataSourceMappings_NIST-800-171-Rev-2.zip](#).

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan NIST 800-171. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit NIST. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [Institut Nasional Standar dan Teknologi \(NIST\)](#)
- [Pusat Sumber Daya Keamanan Komputer NIST](#)
- [AWS Halaman kepatuhan untuk NIST](#)

PCI DSS V3.2.1

AWS Audit Manager menyediakan kerangka standar bawaan yang mendukung Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) v3.2.1.

Note

Untuk informasi tentang PCI DSS v4 dan kerangka kerja Audit Manager yang mendukungnya, lihat [PCI DSS V4.0](#)

Topik

- [Apa itu PCI DSS?](#)
- [Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu PCI DSS?

PCI DSS adalah standar keamanan informasi eksklusif. Ini dikelola oleh [Dewan Standar Keamanan PCI](#), yang didirikan oleh American Express, Discover Financial Services, JCB International, MasterCard Worldwide, dan Visa Inc. PCI DSS berlaku untuk entitas yang menyimpan, memproses, atau mengirimkan data pemegang kartu (CHD) atau data otentikasi sensitif (SAD). Ini termasuk, tetapi tidak terbatas pada, pedagang, prosesor, pengakuisisi, penerbit, dan penyedia layanan. PCI DSS diamanatkan oleh merek kartu dan dikelola oleh Dewan Standar Keamanan Industri Kartu Pembayaran.

AWS disertifikasi sebagai Penyedia Layanan PCI DSS Level 1, yang merupakan tingkat penilaian tertinggi yang tersedia. Penilaian kepatuhan dilakukan oleh Coalfire Systems Inc., sebuah Qualified Security Assessor (QSA) independen. Ringkasan Pengesahan Kepatuhan (AOC) dan Tanggung Jawab PCI DSS tersedia untuk Anda melalui AWS Artifact. Ini adalah portal swalayan untuk akses sesuai permintaan ke laporan AWS kepatuhan. [AWS Artifact Masuk ke Konsol AWS Manajemen](#), atau pelajari lebih lanjut di [Memulai AWS Artifact](#).

Anda dapat mengunduh standar PCI DSS dari Perpustakaan Dokumen [Dewan Standar Keamanan PCI](#).

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka kerja PCI DSS V3.2.1 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan PCI DSS. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat

penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka kerja PCI DSS V3.2.1. Saat tiba waktunya untuk audit, Anda —atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) v3.2.1	38	246	15

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM. Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file [AuditManager_ConfigDataSourceMappings_PCI-DSS-v3.2.1.zip](#).

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan standar PCI DSS. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit PCI DSS. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [Dewan Standar Keamanan PCI](#)
- [Perpustakaan Dokumen Dewan Standar Keamanan PCI](#).
- [AWS Halaman kepatuhan untuk PCI DSS](#)

PCI DSS V4.0

AWS Audit Manager menyediakan kerangka kerja bawaan yang mendukung Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) v4.0.

Note

Untuk informasi tentang PCI DSS v3.2.1 dan kerangka kerja Audit Manager yang mendukungnya, lihat. [PCI DSS V3.2.1](#)

Topik

- [Apa itu PCI DSS?](#)
- [Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu PCI DSS?

Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) adalah standar global yang menyediakan dasar persyaratan teknis dan operasional untuk melindungi data pembayaran. PCI DSS v4.0 adalah evolusi standar berikutnya.

PCI DSS dikembangkan untuk mendorong dan meningkatkan keamanan data akun kartu pembayaran. Ini juga memfasilitasi adopsi luas langkah-langkah keamanan data yang konsisten secara global. Ini memberikan dasar persyaratan teknis dan operasional yang dirancang untuk melindungi data akun. Meskipun dirancang khusus untuk fokus pada lingkungan dengan data akun kartu pembayaran, Anda juga dapat menggunakan PCI DSS untuk melindungi dari ancaman dan mengamankan elemen lain dalam ekosistem pembayaran.

Dewan Standar Keamanan PCI (PCI SSC) memperkenalkan banyak perubahan antara PCI DSS v3.2.1 dan v4.0. Pembaruan ini dibagi menjadi tiga kategori:

1. Persyaratan yang berkembang — Perubahan untuk memastikan bahwa standar tersebut mutakhir dengan ancaman dan teknologi yang muncul, dan perubahan dalam industri pembayaran. Contohnya termasuk persyaratan baru atau modifikasi atau prosedur pengujian, atau penghapusan persyaratan.
2. Klarifikasi atau panduan — Pembaruan kata-kata, penjelasan, definisi, panduan tambahan, atau instruksi untuk meningkatkan pemahaman atau memberikan informasi atau panduan lebih lanjut tentang topik tertentu.
3. Struktur atau format — Reorganisasi konten, termasuk menggabungkan, memisahkan, dan menomori ulang persyaratan untuk menyelaraskan konten.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Note

Framework standar ini menggunakan kontrol terkonsolidasi dari Security Hub CSPM sebagai sumber data. Agar berhasil mengumpulkan bukti dari kontrol terkonsolidasi, pastikan Anda [mengaktifkan pengaturan temuan kontrol terkonsolidasi di Security Hub](#) CSPM. Untuk informasi selengkapnya tentang menggunakan Security Hub sebagai tipe sumber data, lihat [AWS Security Hub CSPM kontrol yang didukung oleh AWS Audit Manager](#).

Anda dapat menggunakan kerangka kerja PCI DSS V4.0 untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan PCI DSS V4.0. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka PCI DSS V4.0. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengeksportnya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) v4.0	40	240	15

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM. Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file [AuditManager_ConfigDataSourceMappings_PCI-DSS-v4.0.zip](#).

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai dengan standar PCI DSS. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit PCI DSS. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [Pusat Sumber Daya PCI DSS v4.0](#)
- [Dewan Standar Keamanan PCI](#)
- [Perpustakaan Dokumen Dewan Standar Keamanan PCI](#)
- [AWS Halaman kepatuhan untuk PCI DSS](#)
- [Standar Keamanan Data Industri Kartu Pembayaran \(PCI DSS\) v4.0 tentang Panduan Kepatuhan AWS](#)

SSAE-18 SOC 2

AWS Audit Manager menyediakan kerangka kerja standar bawaan yang mendukung Laporan Statement on Standards for Attestations Engagement (SSAE) No. 18, Service Organizations Controls (SOC) Report 2.

Topik

- [Apa itu SOC 2?](#)
- [Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Apa itu SOC 2?

SOC 2, didefinisikan oleh [American Institute of Certified Public Accountants](#) (AICPA), adalah nama dari serangkaian laporan yang dihasilkan selama audit. Ini dimaksudkan untuk digunakan oleh organisasi layanan (organisasi yang menyediakan sistem informasi sebagai layanan kepada organisasi lain) untuk mengeluarkan laporan [kontrol internal](#) yang divalidasi atas sistem informasi tersebut kepada pengguna layanan tersebut. Laporan berfokus pada kontrol yang dikelompokkan ke dalam lima kategori yang dikenal sebagai Prinsip Layanan Kepercayaan.

AWS Laporan SOC adalah laporan pemeriksaan pihak ketiga independen yang menunjukkan bagaimana AWS mencapai kontrol dan tujuan kepatuhan utama. Tujuan dari laporan ini adalah untuk membantu Anda dan auditor Anda memahami AWS kontrol yang ditetapkan untuk mendukung operasi dan kepatuhan. Ada lima laporan AWS SOC:

- AWS Laporan SOC 1, tersedia untuk AWS pelanggan dari [AWS Artifact](#).
- AWS Laporan Keamanan, Ketersediaan & Kerahasiaan SOC 2, tersedia untuk AWS pelanggan dari [AWS Artifact](#)
- AWS Laporan Keamanan, Ketersediaan & Kerahasiaan SOC 2 tersedia untuk AWS pelanggan dari [AWS Artifact](#)(cakupan hanya mencakup Amazon DocumentDB).
- AWS Laporan Privasi Tipe I SOC 2, tersedia untuk AWS pelanggan dari [AWS Artifact](#).
- AWS Laporan Keamanan, Ketersediaan & Kerahasiaan SOC 3, [tersedia untuk umum](#) sebagai whitepaper.

Menggunakan kerangka kerja ini untuk mendukung persiapan audit Anda

Anda dapat menggunakan kerangka kerja ini untuk membantu Anda mempersiapkan audit. Kerangka kerja ini mencakup kumpulan kontrol bawaan dengan deskripsi dan prosedur pengujian. Kontrol ini dikelompokkan ke dalam set kontrol sesuai dengan persyaratan SOC 2. Anda juga dapat menyesuaikan kerangka kerja ini dan kontrolnya untuk mendukung audit internal dengan persyaratan khusus.

Dengan menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian Audit Manager dan mulai mengumpulkan bukti yang relevan untuk audit Anda. Setelah Anda membuat penilaian, Audit Manager mulai menilai AWS sumber daya Anda. Ini dilakukan berdasarkan kontrol yang didefinisikan dalam kerangka kerja. Saat tiba waktunya untuk audit, Anda—atau delegasi pilihan Anda—dapat meninjau bukti yang dikumpulkan oleh Audit Manager. Anda juga dapat menelusuri folder bukti dalam penilaian Anda dan memilih bukti mana yang ingin Anda sertakan dalam laporan

penilaian Anda. Atau, jika Anda mengaktifkan pencari bukti, Anda dapat mencari bukti spesifik dan mengekspornya dalam format CSV, atau membuat laporan penilaian dari hasil penelusuran Anda. Either way, Anda dapat menggunakan laporan penilaian ini untuk menunjukkan bahwa kontrol Anda berfungsi sebagaimana dimaksud.

Rincian kerangka kerja adalah sebagai berikut:

Nama kerangka kerja di AWS Audit Manager	Jumlah kontrol otomatis	Jumlah kontrol manual	Jumlah set kontrol
Statement on Standards for Attestations Engagemen t (SSAE) No. 18, Service Organizations Controls (SOC) Report 2	15	46	20

Important

Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Security Hub CSPM, pastikan Anda mengaktifkan semua standar di Security Hub CSPM. Untuk memastikan bahwa kerangka kerja ini mengumpulkan bukti yang diinginkan AWS Config, pastikan Anda mengaktifkan AWS Config aturan yang diperlukan. Untuk meninjau AWS Config aturan yang digunakan sebagai pemetaan sumber data dalam kerangka standar ini, unduh file [AuditManager_ConfigDataSourceMappings_SSAE-NO.-18-SOC-Report-2.zip](#).

Kontrol dalam AWS Audit Manager kerangka kerja ini tidak dimaksudkan untuk memverifikasi apakah sistem Anda sesuai. Selain itu, mereka tidak dapat menjamin bahwa Anda akan lulus audit. AWS Audit Manager tidak secara otomatis memeriksa kontrol prosedural yang memerlukan pengumpulan bukti manual.

Langkah selanjutnya

Untuk petunjuk tentang cara melihat informasi terperinci tentang kerangka kerja ini, termasuk daftar kontrol standar yang dikandungnya, lihat [Meninjau kerangka kerja di AWS Audit Manager](#).

Untuk petunjuk tentang cara membuat penilaian menggunakan kerangka kerja ini, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara menyesuaikan kerangka kerja ini untuk mendukung persyaratan spesifik Anda, lihat [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [AWS Halaman kepatuhan untuk SOC](#)

Jenis sumber data yang didukung untuk bukti otomatis

Saat membuat kontrol kustom di AWS Audit Manager, Anda dapat mengatur kontrol untuk mengumpulkan bukti otomatis dari jenis sumber data berikut:

- AWS CloudTrail
- AWS Security Hub CSPM
- AWS Config
- AWS Panggilan API

Setiap jenis sumber data menawarkan kemampuan berbeda untuk menangkap log aktivitas pengguna, temuan kepatuhan, konfigurasi sumber daya, dan banyak lagi.

Dalam bagian ini Anda dapat mempelajari tentang masing-masing jenis sumber data otomatis ini, dan AWS Security Hub CSPM kontrol, AWS Config aturan, dan panggilan AWS API tertentu yang didukung oleh Audit Manager.

Poin kunci

Tabel berikut memberikan gambaran umum dari setiap jenis sumber data otomatis.

Jenis sumber data	Deskripsi	Frekuensi pengumpulan bukti	Untuk menggunakan jenis sumber data ini...	Ketika kontrol ini aktif dalam penilaian...	Kiat pemecahan masalah terkait
AWS CloudTrail	Melacak aktivitas pengguna tertentu.	Berkelanjutan.	Pilih dari daftar nama acara yang didukung .	Audit Manager memfilter CloudTrail log Anda berdasarkan kata kunci yang Anda pilih. Hasilnya diimpor sebagai bukti aktivitas Pengguna.	Penilaian saya tidak mengumpulkan bukti aktivitas pengguna dari

Jenis sumber data	Deskripsi	Frekuensi pengumpulan bukti	Untuk menggunakan jenis sumber data ini...	Ketika kontrol ini aktif dalam penilaian...	Kiat pemecahan masalah terkait
					AWS CloudTrail !
AWS Config	Menangkap snapshot dari postur keamanan sumber daya Anda dengan melaporkan temuan dari AWS Config.	Berdasarkan pemicu yang didefinisikan dalam AWS Config aturan.	Pilih jenis aturan, lalu pilih aturan. • Untuk aturan terkelola, pilih dari daftar kata kunci aturan terkelola yang didukung. • Untuk aturan khusus, pilih dari daftar aturan yang tersedia.	Manajer Audit mendapatkan temuan untuk aturan ini langsung dari AWS Config. Hasilnya diimpor sebagai bukti pemeriksaan kepatuhan.	Penilaian saya tidak mengumpulkan bukti pemeriksaan an kepatuhan dari AWS Config AWS Config masalah integrasi

Jenis sumber data	Deskripsi	Frekuensi pengumpulan bukti	Untuk menggunakan jenis sumber data ini...	Ketika kontrol ini aktif dalam penilaian...	Kiat pemecahan masalah terkait
AWS Security Hub CSPM	Menangkap snapshot dari postur keamanan sumber daya Anda dengan melaporkan temuan dari Security Hub CSPM.	Berdasarkan jadwal pemeriksaan CSPM Security Hub.	Pilih dari daftar ID kontrol CSPM Security Hub yang didukung .	Audit Manager mendapatkan hasil pemeriksaan keamanan langsung dari Security Hub CSPM. Hasilnya diimpor sebagai bukti pemeriksaan kepatuhan.	Penilaian saya tidak mengumpulkan bukti pemeriksaan kepatuhan dari AWS Security Hub CSPM

Jenis sumber data	Deskripsi	Frekuensi pengumpulan bukti	Untuk menggunakan jenis sumber data ini...	Ketika kontrol ini aktif dalam penilaian...	Kiat pemecahan masalah terkait
AWS Panggil API	Mengambil snapshot konfigurasi sumber daya Anda secara langsung melalui panggilan API ke yang ditentukan Layanan AWS.	Harian, mingguan, atau bulanan.	Pilih dari daftar panggilan API yang didukung , lalu pilih frekuensi pilihan Anda.	Audit Manager membuat panggilan API berdasarkan frekuensi yang Anda tentukan. Respons diimpor sebagai bukti data Konfigurasi.	Penilaian saya tidak mengumpulkan bukti data konfigurasi untuk AWS Panggilan API

Tip

Anda dapat membuat kontrol khusus yang mengumpulkan bukti menggunakan pengelompokan yang telah ditentukan dari sumber data di atas. Pengelompokan sumber data ini dikenal sebagai sumber [ter](#) AWS kelola. Setiap AWS sumber terkelola mewakili kontrol umum atau kontrol inti yang selaras dengan persyaratan kepatuhan umum. Ini memberi Anda cara yang efisien untuk memetakan persyaratan kepatuhan Anda ke kelompok sumber AWS data yang relevan. Untuk melihat kontrol umum yang tersedia, lihat [Menemukan kontrol yang tersedia di AWS Audit Manager](#).

Atau, Anda dapat menggunakan empat jenis sumber data di atas untuk menentukan sumber data kustom Anda sendiri. Ini memberi Anda fleksibilitas untuk mengunggah bukti manual, atau mengumpulkan bukti otomatis dari sumber daya khusus bisnis seperti AWS Config aturan khusus.

Langkah selanjutnya

Untuk mempelajari lebih lanjut tentang sumber data tertentu yang dapat Anda gunakan dalam kontrol kustom Anda, lihat halaman berikut.

- [Aturan AWS Config didukung oleh AWS Audit Manager](#)
- [AWS Security Hub CSPM kontrol didukung oleh AWS Audit Manager](#)
- [AWS Panggilan API didukung oleh AWS Audit Manager](#)
- [AWS CloudTrail nama acara didukung oleh AWS Audit Manager](#)

Aturan AWS Config didukung oleh AWS Audit Manager

Anda dapat menggunakan Audit Manager untuk menangkap AWS Config evaluasi sebagai bukti audit. Saat Anda membuat atau mengedit kontrol kustom, Anda dapat menentukan satu atau lebih AWS Config aturan sebagai pemetaan sumber data untuk pengumpulan bukti. AWS Config melakukan pemeriksaan kepatuhan berdasarkan aturan ini, dan Manajer Audit melaporkan hasilnya sebagai bukti pemeriksaan kepatuhan.

Selain aturan terkelola, Anda juga dapat memetakan aturan kustom Anda ke sumber data kontrol.

Daftar Isi

- [Poin kunci](#)
- [Didukung AWS Config aturan yang dikelola](#)
- [Penggunaan AWS Config aturan khusus dengan Audit Manager](#)
- [Sumber daya tambahan](#)

Poin kunci

- Audit Manager tidak mengumpulkan bukti dari AWS Config aturan [terkait layanan](#), dengan pengecualian aturan terkait layanan dari Paket Kesesuaian dan dari AWS Organizations
- Audit Manager tidak mengelola AWS Config aturan untuk Anda. Sebelum memulai pengumpulan bukti, sebaiknya tinjau parameter AWS Config aturan saat ini. Kemudian, validasi parameter tersebut terhadap persyaratan kerangka kerja yang Anda pilih. Jika diperlukan, Anda dapat [memperbarui parameter aturan AWS Config](#) sehingga selaras dengan persyaratan kerangka

kerja. Ini akan membantu memastikan bahwa penilaian Anda mengumpulkan bukti pemeriksaan kepatuhan yang benar untuk kerangka kerja tersebut.

Misalnya, Anda membuat penilaian untuk CIS v1.2.0. Kerangka kerja ini memiliki kontrol bernama [Pastikan kebijakan kata sandi IAM memerlukan panjang minimum 14 atau lebih](#). Di AWS Config, [aturan](#) iam-password-policy memiliki MinimumPasswordLength parameter yang memeriksa panjang kata sandi. Nilai default untuk parameter ini adalah 14 karakter. Akibatnya, aturan selaras dengan persyaratan kontrol. Jika Anda tidak menggunakan nilai parameter default, pastikan nilai yang Anda gunakan sama dengan atau lebih besar dari persyaratan 14 karakter dari CIS v1.2.0. Anda dapat menemukan detail parameter default untuk setiap aturan terkelola dalam [AWS Config dokumentasi](#).

- Jika Anda perlu memverifikasi apakah AWS Config aturan adalah aturan terkelola atau aturan khusus, Anda dapat melakukannya menggunakan [AWS Config konsol](#). Dari menu navigasi kiri, pilih **Aturan** dan cari aturan di tabel. Jika ini adalah aturan terkelola, kolom **Jenis** menampilkan **AWS dikelola**.

	Name	Remediation action	Type	Compliance
☐	account-part-of-organizations	Not set	AWS managed	✔ Compliant

Didukung AWS Config aturan yang dikelola

Aturan ter AWS Config kelola berikut didukung oleh Audit Manager. Anda dapat menggunakan salah satu kata kunci pengenalan aturan terkelola berikut saat menyiapkan sumber data untuk kontrol kustom. Untuk informasi selengkapnya tentang salah satu aturan terkelola yang tercantum di bawah ini, pilih item dari daftar atau lihat [AWS Config Aturan Ter](#) kelola di Panduan AWS Config Pengguna.

Tip

Saat memilih aturan terkelola di konsol Audit Manager selama pembuatan kontrol kustom, pastikan Anda mencari salah satu kata kunci pengidentifikasi aturan berikut, dan bukan nama aturan. Untuk informasi tentang perbedaan antara nama aturan dan pengidentifikasi aturan, dan cara menemukan pengidentifikasi untuk aturan terkelola, lihat [bagian Pemecahan masalah](#) pada panduan pengguna ini.

Kata kunci aturan AWS Config terkelola yang didukung

- [KUNCI_AKSES_DIPUTAR](#)
- [AKUN_BAGIAN_ORGANISASI](#)
- [ACM_CERTIFICATE_EXPIRATION_CHECK](#)
- [ACM_CERTIFICATE_RSA_CHECK](#)
- [ALB_DESYNC_MODE_CHECK](#)
- [ALB_HTTP_DROP_INVALID_HEADER_ENABLED](#)
- [ALB_HTTP_KE_HTTPS_PENGALIHAN_PERIKSA](#)
- [ALB_WAF_ENABLED](#)
- [API_GW_BERASOSIASI DENGAN WAF](#)
- [API_GW_CACHE_DIAKTIFKAN DAN ENKRIPSI](#)
- [API_GW_ENDPOINT_TYPE_CHECK](#)
- [API_GW_EXECUTION_LOGGING_ENABLED](#)
- [API_GW_SSL_ENABLED](#)
- [API_GW_XRAY_DIAKTIFKAN](#)
- [API_GWV2_ACCESS_LOGS_ENABLED](#)
- [API_GWV2_AUTHORIZATION_TYPE_CONFIGURED](#)
- [DISETUJUKAN_AMIS_OLEH_ID](#)
- [DISETUJUKAN_AMIS_BY_TAG](#)
- [APPSYNC_BERASOSIASI DENGAN WAF](#)
- [APPSYNC_CACHE_ENKRIPTION_AT_REST](#)
- [APPSYNC_LOGGING_DIAKTIFKAN](#)
- [AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED](#)
- [AURORA_MYSQL_BACKTRACKING_ENABLED](#)
- [AURORA_RESOURCES_DILINDUNGI OLEH CADANGAN_RENCANA](#)
- [PENYIMBANGAN ULANG KAPASITAS PENSKALAN OTOMATIS](#)
- [AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED](#)
- [AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT](#)
- [AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED](#)
- [PENSKALAN OTOMATIS_LAUNCHCONFIG_REQUIRES_IMDSV2](#)

Kata kunci aturan AWS Config terkelola yang didukung

- [TEMPLATE PELUNCURAN SKALA OTOMATIS](#)
- [PENSKALAAN OTOMATIS MULTIPLE_AZ](#)
- [PENSKALAAN OTOMATIS MULTIPLE_INSTANCE_TYPES](#)
- [CADANGAN_RENCANA_FREKUENSI_MIN_DAN_RETENTION_CHECK_MIN](#)
- [BACKUP_RECOVERY_POINT_ENCRYPTED](#)
- [CADANGAN_PEMULIHAN_POINT_MANUAL_PENGHAPUSAN_DISABLED](#)
- [BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK](#)
- [BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED](#)
- [CLB_DESYNC_MODE_CHECK](#)
- [CLB_MULTIPLE_AZ](#)
- [CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED](#)
- [CLOUD_TRAIL_DIAKTIFKAN](#)
- [CLOUD_TRAIL_ENKRIPTAN_DIAKTIFKAN](#)
- [CLOUD_TRAIL_LOG_FILE_VALIDATION_DIAKTIFKAN](#)
- [CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK](#)
- [CLOUDFORMATION_STACK_NOTIFICATION_CHECK](#)
- [CLOUDFRONT_ACCESSLOGS_ENABLED](#)
- [CLOUDFRONT_BERASOSIASI DENGAN_WAF](#)
- [CLOUDFRONT_CUSTOM_SSL_SERTIFIKAT](#)
- [CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED](#)
- [CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS](#)
- [CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED](#)
- [CLOUDFRONT_ORIGIN_FAILOVER_ENABLED](#)
- [CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED](#)
- [CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET](#)
- [CLOUDFRONT_SECURITY_POLICY_CHECK](#)
- [CLOUDFRONT_SNI_DIAKTIFKAN](#)
- [CLOUDFRONT_TRAFFIC_KE_ASLI_ENKRIPSI](#)
- [CLOUDFRONT_VIEWER_POLICY_HTTPS](#)

Kata kunci aturan AWS Config terkelola yang didukung

- [CLOUDTRAIL_S3_DATAEVENTS_ENABLED](#)
- [CLOUDTRAIL_SECURITY_TRAIL_ENABLED](#)
- [CLOUDWATCH_ALARM_ACTION_CHECK](#)
- [CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK](#)
- [CLOUDWATCH_ALARM_RESOURCE_CHECK](#)
- [CLOUDWATCH_ALARM_PENGATURAN_PERIKSA](#)
- [CLOUDWATCH_LOG_GROUP_ENKRIPSI](#)
- [CMK_BACKING_KEY_ROTATION_ENABLED](#)
- [CODEBUILD_PROJECT_ARTIFACT_ENKRIPSI](#)
- [CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK](#)
- [CODEBUILD_PROJECT_ENVVAR_AWSCRED_CHECK](#)
- [CODEBUILD_PROJECT_LOGGING_DIAKTIFKAN](#)
- [CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED](#)
- [CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK](#)
- [CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED](#)
- [CODEDEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED](#)
- [CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED](#)
- [CODEPIPELINE_DEPLOYMENT_COUNT_CHECK](#)
- [CODEPIPELINE_REGION_FANOUT_CHECK](#)
- [CUSTOM_SCHEMA_REGISTRY_POLICY_TERLAMPIR](#)
- [CW_LOGGROUP_RETENTION_PERIODE_CHECK](#)
- [DAX_ENKRIPTION_DIAKTIFKAN](#)
- [DB_INSTANCE_BACKUP_DIAKTIFKAN](#)
- [PERSEWAAN INSTANSI YANG DIINGINKAN](#)
- [TIPE_INSTANCE YANG DIINGINKAN](#)
- [DMS_REPLIKASI_TIDAK_PUBLIK](#)
- [DYNAMODB_AUTOSCALING_ENABLED](#)
- [DYNAMODB_DALAM_CADANGAN_RENCANA](#)
- [DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED](#)

Kata kunci aturan AWS Config terkelola yang didukung

- [DYNAMODB_PITR_ENABLED](#)
- [DYNAMODB_RESOURCES_DILINDUNGI_OLEH_CADANGAN_RENCANA](#)
- [DYNAMODB_TABLE_ENKRIPTED_KMS](#)
- [DYNAMODB_TABLE_ENKRIPTION_DIAKTIFKAN](#)
- [DYNAMODB_THROUGHPUT_LIMIT_CHECK](#)
- [EBS_DI_CADANGAN_RENCANA](#)
- [EBS_LAST_BACKUP_RECOVERY_POINT_DIBUAT](#)
- [EBS_INSTANCE YANG DIOPTIMALKAN](#)
- [EBS_RESOURCES_DILINDUNGI_OLEH_CADANGAN_RENCANA](#)
- [EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK](#)
- [EC2_CLIENT_VPN_NOT_OTORIZE_ALL](#)
- [EC2_EBS_ENKRIPTION_BY_DEFAULT](#)
- [EC2_IMDSV2_PERIKSA](#)
- [EC2_INSTANCE_DETAILED_MONITORING_DIAKTIFKAN](#)
- [EC2_INSTANCE_DIKELOLA_OLEH_SSM](#)
- [EC2_INSTANCE_MULTIPLE_ENI_CHECK](#)
- [EC2_INSTANCE_NO_PUBLIC_IP](#)
- [EC2_INSTANCE_PROFILE_TERLAMPIR](#)
- [EC2_LAST_BACKUP_RECOVERY_POINT_DIBUAT](#)
- [EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED](#)
- [EC2_MANAGEDINSTANCE_APPLICATIONS_DAFTAR HITAM](#)
- [EC2_MANAGEDINSTANCE_APLIKASI_DIPERLUKAN](#)
- [EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK](#)
- [EC2_MANAGEDINSTANCE_INVENTORY_DAFTAR HITAM](#)
- [EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK](#)
- [EC2_MANAGEDINSTANCE_PLATFORM_CHECK](#)
- [EC2_NO_AMAZON_KEY_PAIR](#)
- [EC2_PARAVIRTUAL_INSTANCE_CHECK](#)
- [EC2_RESOURCES_DILINDUNGI_OLEH_CADANGAN_RENCANA](#)

Kata kunci aturan AWS Config terkelola yang didukung

- [EC2_KEAMANAN_GRP_TERLAMPIRAN_KE_ENI](#)
- [EC2_SECURITY_GROUP_TERLAMPIRAN_KE_ENI_PERIODIK](#)
- [EC2_INSTANCE YANG DIHENTIKAN](#)
- [EC2_TOKEN_HOP_LIMIT_CHECK](#)
- [EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED](#)
- [EC2_VOLUME_INUSE_CHECK](#)
- [ECR_PRIVATE_IMAGE_SCANNING_DIAKTIFKAN](#)
- [ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED](#)
- [ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED](#)
- [ECS_AWSVPC_NETWORKING_ENABLED](#)
- [ECS_CONTAINER_INSIGHTS_ENABLED](#)
- [ECS_CONTAINERS_NONPRIVILEGED](#)
- [ECS_CONTAINERS_READONLY_ACCESS](#)
- [ECS_FARGATE_VERSION_PLATFORM TERBARU](#)
- [ECS_NO_RAHASIA LINGKUNGAN](#)
- [ECS_TASK_DEFINISI_LOG_KONFIGURASI_KONFIGURASI](#)
- [ECS_TASK_DEFINISI_MEMORY_HARD_LIMIT](#)
- [ECS_TASK_DEFINISI_NONROOT_USER](#)
- [ECS_TASK_DEFINISI_PID_MODE_CHECK](#)
- [ECS_TASK_DEFINISI_USER_UNTUK_MODE_CHECK](#)
- [EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY](#)
- [EFS_ACCESS_POINT_ENFORCE_IDENTITAS PENGGUNA](#)
- [EFS_ENKRIPTE PERIKSA](#)
- [EFS_DI CADANGAN RENCANA](#)
- [EFS_BACKUP_LAST_RECOVERY_POINT_DIBUAT](#)
- [EFS_RESOURCES_DILINDUNGI OLEH CADANGAN RENCANA](#)
- [EIP_TERLAMPIR](#)
- [EKS_CLUSTER_LOGGING_DIAKTIFKAN](#)
- [EKS_CLUSTER_VERSI TERLAMA DIDUKUNG](#)

Kata kunci aturan AWS Config terkelola yang didukung

- [EKS_CLUSTER_VERSI_DIDUKUNG](#)
- [EKS_ENDPOINT_NO_ACCESS_PUBLIC](#)
- [EKS_SECRETS_ENKRIPSI](#)
- [ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH](#)
- [ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED](#)
- [ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK](#)
- [ELASTICACHE_RBAC_AUTH_ENABLED](#)
- [ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK](#)
- [ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED](#)
- [ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST](#)
- [ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT](#)
- [ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED](#)
- [ELASTICACHE_SUBNET_GROUP_CHECK](#)
- [VERSI_ENGINE_ELASTICACHE_DIDUKUNG](#)
- [ELASTICSEARCH_ENCRYPTED_AT_REST](#)
- [ELASTICSEARCH_DI_VPC_ONLY](#)
- [ELASTICSEARCH_LOGS_TO_CLOUDWATCH](#)
- [ELASTICSEARCH_NODE_TO_NODE_ENKRIPTION_CHECK](#)
- [ELB_ACM_SERTIFIKAT_DIPERLUKAN](#)
- [ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED](#)
- [ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK](#)
- [ELB_DELETION_PROTECTION_ENABLED](#)
- [ELB_LOGGING_DIAKTIFKAN](#)
- [ELB_DEFINED_KEAMANAN_KEBIJAKAN_SSL_PERIKSA](#)
- [ELB_TLS_HTTPS_PENDENGAR_SAJA](#)
- [ELBV2_ACM_SERTIFIKAT_DIPERLUKAN](#)
- [ELBV2_MULTIPLE_AZ](#)
- [EMR_KERBEROS_ENABLED](#)
- [EMR_MASTER_NO_PUBLIC_IP](#)

Kata kunci aturan AWS Config terkelola yang didukung

- [VOLUME TERENKRIPSI](#)
- [FMS_SHIELD_RESOURCE_POLICY_CHECK](#)
- [FMS_WEBACL_RESOURCE_POLICY_CHECK](#)
- [FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK](#)
- [FSX_LAST_BACKUP_RECOVERY_POINT_DIBUAT](#)
- [FSX_RESOURCES_DILINDUNGI_OLEH_CADANGAN_RENCANA](#)
- [GUARDDUT_DIAKTIFKAN_TERPUSAT](#)
- [PENJAGA_NON_ARSIP_TEMUAN](#)
- [IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS](#)
- [IAM_GROUP_HAS_USER_CHECK](#)
- [IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS](#)
- [IAM_NO_INLINE_POLICY_CHECK](#)
- [IAM_PASSWORD_POLICY](#)
- [IAM_POLICY_BLACKLISTED_CHECK](#)
- [IAM_POLICY_DALAM_DIGUNAKAN](#)
- [IAM_POLICY_NO_STATEMENT_DENGAN_ADMIN_ACCESS](#)
- [IAM_POLICY_NO_STATEMENT_DENGAN_FULL_ACCESS](#)
- [IAM_ROLE_MANAGED_POLICY_CHECK](#)
- [IAM_ROOT_ACCESS_KEY_CHECK](#)
- [IAM_USER_GROUP_MEMBERSHIP_CHECK](#)
- [IAM_USER_MFA_ENABLED](#)
- [IAM_USER_NO_POLICIES_CHECK](#)
- [IAM_USER_UNUSED_CREDENTIALS_CHECK](#)
- [INCOMING_SSH_DISABLED](#)
- [INSTANCES_DALAM_VPC](#)
- [KINESIS_STREAM_ENCRYPTED](#)
- [INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY](#)
- [KMS_CMK_TIDAK_TERJADWAL_UNTUK_PENGHAPUSAN](#)
- [LAMBDA_CONCURRENCY_CHECK](#)

Kata kunci aturan AWS Config terkelola yang didukung

- [LAMBDA_DLQ_PERIKSA](#)
- [LAMBDA_FUNGSI_AKSES_PUBLIK_DILARANG](#)
- [LAMBDA_FUNGSI_PENGATURAN_PERIKSA](#)
- [LAMBDA_INSIDE_VPC](#)
- [LAMBDA_VPC_MULTI_AZ_CHECK](#)
- [MACIE_STATUS_CHECK](#)
- [MFA_ENABLED_UNTUK_IAM_CONSOLE_ACCESS](#)
- [MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED](#)
- [MQ_CLOUDWATCH_AUDIT_LOGGING_DIAKTIFKAN](#)
- [MQ_NO_PUBLIC_ACCESS](#)
- [MULTI_REGION_CLOUD_TRAIL_ENABLED](#)
- [NACL_NO_UNRESTRICTED_SSH_RDP](#)
- [NETFW_LOGGING_DIAKTIFKAN](#)
- [NETFW_MULTI_AZ_DIAKTIFKAN](#)
- [NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS](#)
- [NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS](#)
- [NETFW_POLICY_RULE_GROUP_ASSOCIATED](#)
- [NETFW_STATELESS_RULE_GROUP_NOT_EMPTY](#)
- [NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED](#)
- [NO_ROUTE_UNRESTRICTED_KE_IGW](#)
- [OPENSEARCH_ACCESS_CONTROL_DIAKTIFKAN](#)
- [OPENSEARCH_AUDIT_LOGGING_DIAKTIFKAN](#)
- [OPENSEARCH_DATA_NODE_FAULT_TOLERANCE](#)
- [OPENSEARCH_ENCRYPTED_AT_REST](#)
- [OPENSEARCH_HTTPS_REQUIRED](#)
- [OPENSEARCH_DI_VPC_ONLY](#)
- [OPENSEARCH_LOGS_TO_CLOUDWATCH](#)
- [OPENSEARCH_NODE_TO_NODE_ENKRIPTION_CHECK](#)
- [RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED](#)

Kata kunci aturan AWS Config terkelola yang didukung

- [RDS_CLUSTER_DEFAULT_ADMIN_CHECK](#)
- [RDS_CLUSTER_PENGHAPUSAN_PROTEKTION_DIAKTIFKAN](#)
- [RDS_CLUSTER_IAM_AUTHENTIKAN_DIAKTIFKAN](#)
- [RDS_CLUSTER_MULTI_AZ_ENABLED](#)
- [RDS_DB_GRPUP_SECURITY_NOT_DIIZINKAN](#)
- [RDS_ENHANCED_MONITORING_DIAKTIFKAN](#)
- [RDS_DALAM_CADANGAN_RENCANA](#)
- [RDS_INSTANCE_DEFAULT_ADMIN_CHECK](#)
- [RDS_INSTANCE_PENGHAPUSAN_PROTEKTION_DIAKTIFKAN](#)
- [RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED](#)
- [RDS_INSTANCE_PUBLIC_ACCESS_CHECK](#)
- [RDS_LAST_BACKUP_RECOVERY_POINT_CREATED](#)
- [RDS_LOGGING_DIAKTIFKAN](#)
- [RDS_MULTI_AZ_DUKUNGAN](#)
- [RDS_RESOURCES_DILINDUNGI_OLEH_CADANGAN_RENCANA](#)
- [RDS_SNAPSHOT_ENKRIPSI](#)
- [RDS_SNAPSHOTS_PUBLIC_DILARANG](#)
- [RDS_STORAGE_ENCRYPTION](#)
- [REDSHIFT_BACKUP_DIAKTIFKAN](#)
- [REDSHIFT_REQUIRE_TLS_SSL](#)
- [REDSHIFT_CLUSTER_CONFIGURATION_CHECK](#)
- [REDSHIFT_CLUSTER_PENGATURAN PEMELIHARAAN_PERIKSA](#)
- [REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK](#)
- [REDSHIFT_AUDIT_LOGGING_DIAKTIFKAN](#)
- [REDSHIFT_CLUSTER_KMS_ENABLED](#)
- [REDSHIFT_DEFAULT_ADMIN_CHECK](#)
- [REDSHIFT_DEFAULT_DB_NAME_CHECK](#)
- [REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED](#)
- [TAG YANG DIWAJIBKAN](#)

Kata kunci aturan AWS Config terkelola yang didukung

- [LALU LINTAS MASUK TERBATASI](#)
- [ROOT_ACCOUNT_HARDWARE_MFA_ENABLED](#)
- [ROOT_ACCOUNT_MFA_ENABLED](#)
- [S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC](#)
- [S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS](#)
- [S3_BUCKET_ACL_DILARANG](#)
- [S3_BUCKET_BLACKLISTED_ACTIONS_DILARANG](#)
- [S3_BUCKET_DEFAULT_LOCK_ENABLED](#)
- [S3_BUCKET_LEVEL_PUBLIC_ACCESS_DILARANG](#)
- [S3_BUCKET_LOGGING_DIAKTIFKAN](#)
- [S3_BUCKET_POLICY_GRANTEE_CHECK](#)
- [S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE](#)
- [S3_BUCKET_PUBLIC_READ_FORBIDDEN](#)
- [S3_BUCKET_PUBLIC_WRITE_DILARANG](#)
- [S3_BUCKET_REPLICATION_ENABLED](#)
- [S3_BUCKET_SERVER_SIDE_ENKRIPTION_DIAKTIFKAN](#)
- [S3_BUCKET_SSL_REQUESTS_ONLY](#)
- [S3_BUCKET_VERSION_DIAKTIFKAN](#)
- [S3_DEFAULT_ENKRIPTION_KMS](#)
- [S3_EVENT_NOTIFICATIONS_ENABLED](#)
- [S3_LAST_BACKUP_RECOVERY_POINT_CREATED](#)
- [S3_LIFECYCLE_POLICY_CHECK](#)
- [S3_RESOURCES_DILINDUNGI_OLEH_CADANGAN_RENCANA](#)
- [S3_VERSION_LIFECYCLE_POLICY_CHECK](#)
- [SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED](#)
- [SAGEMAKER_NOTEBOOK_INSTANCE_DALAM_VPC](#)
- [SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED](#)
- [SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK](#)
- [SAGEMAKER_NOTEBOOK_NO_ACCESS_DIRECT INTERNET](#)

Kata kunci aturan AWS Config terkelola yang didukung

- [SECRETSMANAGER_ROTATION_DIAKTIFKAN_PERIKSA](#)
- [SECRETSMANAGER_TERJADWAL_ROTATION_SUCCESS_CHECK](#)
- [SECRETSMANAGER_SECRET_PERIODIS_ROTASI](#)
- [SECRETSMANAGER_SECRET_TIDAK DIGUNAKAN](#)
- [SECRETSMANAGER_MENGGUNAKAN_CMK](#)
- [KEAMANAN_INFORMASI_AKUN_DISEDIAKAN](#)
- [SECURITYHUB_ENABLED](#)
- [SERVICE_VPC_ENDPOINT_ENABLED](#)
- [SES_MALWARE_SCANNING_DIAKTIFKAN](#)
- [SHIELD_ADVANCED_ENABLED_AUTORENEW](#)
- [SHIELD_DRT_AKSES](#)
- [SNS_ENKRIPTED_KMS](#)
- [SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED](#)
- [SSM_DOKUMENT_BUKAN_PUBLIK](#)
- [LANGKAH_FUNGSI_STATE_MACHINE_LOGGING_ENABLED](#)
- [STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_DIBUAT](#)
- [STORAGEGATEWAY_RESOURCES_DILINDUNGI OLEH CADANGAN_RENCANA](#)
- [SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED](#)
- [VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED](#)
- [SUMBER DAYA MESIN VIRTUAL_DILINDUNGI OLEH BACKUP_PLAN](#)
- [VPC_DEFAULT_SECURITY_GROUP_TERTUTUP](#)
- [VPC_FLOW_LOGS_DIAKTIFKAN](#)
- [VPC_NETWORK_ACL_UNUSED_CHECK](#)
- [VPC_PEERING_DNS_RESOLUTION_CHECK](#)
- [VPC_SG_OPEN_ONLY_TO_PORTS YANG DIOTORISASI](#)
- [VPC_VPN_2_TUNNELS_UP](#)
- [WAF_CLASSIC_LOGGING_DIAKTIFKAN](#)
- [WAF_GLOBAL_RULEGROUP_TIDAK_KOSONG](#)
- [WAF_GLOBAL_RULE_TIDAK_KOSONG](#)

Kata kunci aturan AWS Config terkelola yang didukung

- [WAF_GLOBAL_WEBACL_TIDAK_KOSONG](#)
- [WAF_REGIONAL_RULEGROUP_NOT_EMPTY](#)
- [WAF_REGIONAL_RULE_TIDAK_KOSONG](#)
- [WAF_REGIONAL_WEBACL_TIDAK_KOSONG](#)
- [WAFV2_LOGGING_ENABLED](#)
- [WAFV2_RULEGROUP_NOT_EMPTY](#)
- [WAFV2_WEBACL_NOT_EMPTY](#)

Penggunaan AWS Config aturan khusus dengan Audit Manager

Anda dapat menggunakan aturan AWS Config khusus sebagai sumber data untuk pelaporan audit. Ketika kontrol memiliki sumber data yang dipetakan ke AWS Config aturan, Audit Manager menambahkan evaluasi yang dibuat oleh AWS Config aturan.

Aturan kustom yang dapat Anda gunakan bergantung pada Akun AWS yang Anda gunakan untuk masuk ke Audit Manager. Jika Anda dapat mengakses aturan khusus di AWS Config, Anda dapat menggunakannya sebagai pemetaan sumber data di Audit Manager.

- Untuk individu Akun AWS — Anda dapat menggunakan salah satu aturan khusus yang Anda buat dengan akun Anda.
- Untuk akun yang merupakan bagian dari organisasi — Keduanya, Anda dapat menggunakan salah satu aturan kustom tingkat anggota Anda. Atau, Anda dapat menggunakan salah satu aturan kustom tingkat organisasi yang tersedia untuk Anda di AWS Config

Setelah Anda memetakan aturan kustom Anda sebagai sumber data untuk kontrol, Anda dapat menambahkan kontrol tersebut ke kerangka kerja khusus di Audit Manager.

Sumber daya tambahan

- Untuk menemukan bantuan dengan masalah untuk jenis sumber data ini, lihat [Penilaian saya tidak mengumpulkan bukti pemeriksaan kepatuhan dari AWS Config](#) dan masalah [AWS Config integrasi](#).
- Untuk membuat kontrol kustom menggunakan jenis sumber data ini, lihat [Membuat kontrol khusus di AWS Audit Manager](#).

- Untuk membuat kerangka kerja khusus yang menggunakan kontrol kustom Anda, lihat [Membuat kerangka kerja khusus di AWS Audit Manager](#).
- Untuk menambahkan kontrol kustom Anda ke kerangka kustom yang ada, lihat [Mengedit kerangka kerja khusus di AWS Audit Manager](#).
- Untuk membuat aturan khusus di AWS Config, lihat [Mengembangkan aturan khusus untuk AWS Config](#) di Panduan Peng AWS Config embang.

AWS Security Hub CSPM kontrol didukung oleh AWS Audit Manager

Anda dapat menggunakan Audit Manager untuk menangkap temuan Security Hub CSPM sebagai bukti untuk audit. Saat membuat atau mengedit kontrol kustom, Anda dapat menentukan satu atau beberapa kontrol CSPM Hub Keamanan sebagai pemetaan sumber data untuk pengumpulan bukti. Security Hub CSPM melakukan pemeriksaan kepatuhan berdasarkan kontrol ini, dan Audit Manager melaporkan hasilnya sebagai bukti pemeriksaan kepatuhan.

Daftar Isi

- [Poin kunci](#)
- [Kontrol CSPM Security Hub yang didukung](#)
- [Sumber daya tambahan](#)

Poin kunci

- Audit Manager tidak mengumpulkan bukti dari AWS Config aturan [terkait layanan yang dibuat oleh Security Hub CSPM](#).
- Pada tanggal 9 November 2022, Security Hub CSPM meluncurkan pemeriksaan keamanan otomatis yang selaras dengan persyaratan Benchmark Foundation Center for Internet Security (CIS) AWS versi 1.4.0, Level 1 dan 2 (CIS v1.4.0). Di Security Hub CSPM, standar [CIS v1.4.0](#) didukung selain standar [CIS v1.2.0](#).
- Sebaiknya aktifkan [setelan temuan kontrol](#) konsolidasi di Security Hub CSPM jika belum diaktifkan. Jika Anda mengaktifkan Security Hub CSPM pada atau setelah 23 Februari 2023, pengaturan ini diaktifkan secara default.

Ketika temuan konsolidasi diaktifkan, Security Hub CSPM menghasilkan satu temuan untuk setiap pemeriksaan keamanan (bahkan ketika pemeriksaan yang sama berlaku untuk beberapa standar). Setiap temuan Security Hub CSPM dikumpulkan sebagai satu penilaian sumber daya unik di Audit Manager. Akibatnya, temuan konsolidasi menghasilkan penurunan total penilaian sumber daya unik yang dilakukan Audit Manager untuk temuan Security Hub CSPM. Untuk alasan ini, menggunakan temuan konsolidasi seringkali dapat mengakibatkan pengurangan biaya penggunaan Manajer Audit Anda, tanpa mengorbankan kualitas dan ketersediaan bukti. Untuk informasi lebih lanjut tentang harga, lihat [AWS Audit Manager Harga](#).

Contoh bukti saat temuan konsolidasi dihidupkan atau dimatikan

Contoh berikut menunjukkan perbandingan cara Audit Manager mengumpulkan dan menyajikan bukti tergantung pada setelan CSPM Security Hub Anda.

When consolidated findings is turned on

Katakanlah Anda telah mengaktifkan tiga standar keamanan berikut di Security Hub CSPM: AWS FSBP, PCI DSS, dan CIS Benchmark v1.2.0.

- Ketiga standar ini menggunakan control ([IAM.4](#)) yang sama dengan AWS Config aturan dasar yang sama ([iam-ro](#) ot-access-key-check).
- Karena pengaturan temuan konsolidasi di aktifkan, Security Hub CSPM menghasilkan satu temuan tunggal untuk kontrol ini.
- Security Hub CSPM mengirimkan temuan konsolidasi ke Audit Manager untuk kontrol ini.
- Temuan konsolidasi dihitung sebagai satu penilaian sumber daya unik di Audit Manager. Akibatnya, satu bukti ditambahkan ke penilaian Anda.

Berikut adalah contoh bagaimana bukti itu mungkin terlihat:

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/finding/09876543-p0o9-i8u7-y6t5-098765432109",
  "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-west-2",
```

```

"GeneratorId": "security-control/IAM.4",
"AwsAccountId": "111122223333",
"Types": [
  "Software and Configuration Checks/Industry and Regulatory Standards"
],
"FirstObservedAt": "2023-10-25T11:32:24.861Z",
"LastObservedAt": "2023-11-02T11:59:19.546Z",
"CreatedAt": "2023-10-25T11:32:24.861Z",
"UpdatedAt": "2023-11-02T11:59:15.127Z",
"Severity": {
  "Label": "INFORMATIONAL",
  "Normalized": 0,
  "Original": "INFORMATIONAL"
},
"Title": "IAM root user access key should not exist",
"Description": "This AWS control checks whether the root user access key is
available.",
"Remediation": {
  "Recommendation": {
    "Text": "For information on how to correct this issue, consult the AWS
Security Hub controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
  }
},
"ProductFields": {
  "RelatedAWSResources:0/name": "securityhub-iam-root-access-key-
check-000270f5",
  "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
  "aws/securityhub/ProductName": "Security Hub",
  "aws/securityhub/CompanyName": "AWS",
  "Resources:0/Id": "arn:aws:iam::111122223333:root",
  "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-2::product/aws/
securityhub/arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109"
},
"Resources": [{
  "Type": "AwsAccount",
  "Id": "AWS:::Account:111122223333",
  "Partition": "aws",
  "Region": "us-west-2"
}],
"Compliance": {
  "Status": "PASSED",

```

```

    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v1.2.0/1.12"
    ],
    "SecurityControlId": "IAM.4",
    "AssociatedStandards": [{
      "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
    },
    {
      "StandardsId": "standards/aws-foundational-security-best-practices/
v/1.0.0"
    }
  ]
},
"WorkflowState": "NEW",
"Workflow": {
  "Status": "RESOLVED"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {
    "Label": "INFORMATIONAL",
    "Original": "INFORMATIONAL"
  },
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ]
},
"ProcessedAt": "2023-11-02T11:59:20.980Z"
}

```

When consolidated findings is turned off

Katakanlah Anda telah mengaktifkan tiga standar keamanan berikut di Security Hub CSPM: AWS FSBP, PCI DSS, dan CIS Benchmark v1.2.0.

- Ketiga standar ini menggunakan control ([IAM.4](#)) yang sama dengan AWS Config aturan dasar yang sama ([iam-ro](#) ot-access-key-check).
- Karena pengaturan temuan konsolidasi di matikan, Security Hub CSPM menghasilkan temuan terpisah per pemeriksaan keamanan untuk setiap standar yang diaktifkan (dalam hal ini, tiga temuan).
- Security Hub CSPM mengirimkan tiga temuan khusus standar terpisah ke Audit Manager untuk kontrol ini.

- Ketiga temuan tersebut dihitung sebagai tiga penilaian sumber daya unik di Audit Manager. Akibatnya, tiga bukti terpisah ditambahkan ke penilaian Anda.

Berikut adalah contoh bagaimana bukti itu mungkin terlihat. Perhatikan bahwa dalam contoh ini, masing-masing dari tiga payload berikut memiliki ID kontrol keamanan yang sama (*SecurityControlId*: "IAM.4"). Untuk alasan ini, kontrol penilaian yang mengumpulkan bukti ini di Audit Manager (IAM.4) menerima tiga bukti terpisah ketika temuan berikut datang dari Security Hub CSPM.

Bukti untuk IAM.4 (FSBP)

```
{
  "version": "0",
  "id": "12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type": "Security Hub Findings - Imported",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2023-10-27T18:55:59Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/Lambda.1/finding/b5e68d5d-43c3-46c8-902d-51cb0d4da568"
  ],
  "detail": {
    "findings": [
      {
        "SchemaVersion": "2018-10-08",
        "Id": "arn:aws:securityhub:us-west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-a78f-3cbe9402d17d",
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/securityhub",
        "ProductName": "Security Hub",
        "CompanyName": "AWS",
        "Region": "us-west-2",
        "GeneratorId": "aws-foundational-security-best-practices/v/1.0.0/IAM.4",
        "AwsAccountId": "111122223333",
        "Types": [
          "Software and Configuration Checks/Industry and Regulatory Standards/AWS-Foundational-Security-Best-Practices"
        ],
        "FirstObservedAt": "2020-10-05T19:18:47.848Z",
```

```

    "LastObservedAt": "2023-11-01T14:12:04.106Z",
    "CreatedAt": "2020-10-05T19:18:47.848Z",
    "UpdatedAt": "2023-11-01T14:11:53.720Z",
    "Severity": {
      "Product": 0,
      "Label": "INFORMATIONAL",
      "Normalized": 0,
      "Original": "INFORMATIONAL"
    },
    "Title": "IAM.4 IAM root user access key should not exist",
    "Description": "This AWS control checks whether the root user access key is available.",
    "Remediation": {
      "Recommendation": {
        "Text": "For information on how to correct this issue, consult the AWS Security Hub controls documentation.",
        "Url": "https://docs.aws.amazon.com/console/securityhub/IAM.4/remediation"
      }
    },
    "ProductFields": {
      "StandardsArn": "arn:aws:securityhub::standards/aws-foundational-security-best-practices/v/1.0.0",
      "StandardsSubscriptionArn": "arn:aws:securityhub:us-west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0",
      "ControlId": "IAM.4",
      "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/IAM.4/remediation",
      "RelatedAWSResources:0/name": "securityhub-iam-root-access-key-check-67cbb1c4",
      "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
      "StandardsControlArn": "arn:aws:securityhub:us-west-2:111122223333:control/aws-foundational-security-best-practices/v/1.0.0/IAM.4",
      "aws/securityhub/ProductName": "Security Hub",
      "aws/securityhub/CompanyName": "AWS",
      "Resources:0/Id": "arn:aws:iam::111122223333:root",
      "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-a78f-3cbe9402d17d"
    },
    "Resources": [
      {
        "Type": "AwsAccount",

```

```

        "Id": "AWS:::Account:111122223333",
        "Partition": "aws",
        "Region": "us-west-2"
    },
    ],
    "Compliance": {
        "Status": "PASSED",
        "SecurityControlId": "IAM.4",
        "AssociatedStandards": [
            {
                "StandardsId": "standards/aws-foundational-security-best-
practices/v/1.0.0"
            }
        ]
    },
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "RESOLVED"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "INFORMATIONAL",
            "Original": "INFORMATIONAL"
        },
        "Types": [
            "Software and Configuration Checks/Industry and Regulatory
Standards/AWS-Foundational-Security-Best-Practices"
        ]
    },
    "ProcessedAt": "2023-11-01T14:12:07.395Z"
}
]
}
}

```

Bukti untuk IAM.4 (CIS 1.2)

```

{
  "version": "0",
  "id": "12345678-1q2w-3e4r-5t6y-123456789012",

```

```

"detail-type":"Security Hub Findings - Imported",
"source":"aws.securityhub",
"account":"111122223333",
"time":"2023-10-27T18:55:59Z",
"region":"us-west-2",
"resources":[
  "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
],
"detail":{
  "findings":[
    {
      "SchemaVersion":"2018-10-08",
      "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23",
      "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
      "ProductName":"Security Hub",
      "CompanyName":"AWS",
      "Region":"us-west-2",
      "GeneratorId":"arn:aws:securityhub::ruleset/cis-aws-foundations-
benchmark/v/1.2.0/rule/1.12",
      "AwsAccountId":"111122223333",
      "Types":[
        "Software and Configuration Checks/Industry and Regulatory Standards/
CIS AWS Foundations Benchmark"
      ],
      "FirstObservedAt":"2020-10-05T19:18:47.775Z",
      "LastObservedAt":"2023-11-01T14:12:07.989Z",
      "CreatedAt":"2020-10-05T19:18:47.775Z",
      "UpdatedAt":"2023-11-01T14:11:53.720Z",
      "Severity":{
        "Product":0,
        "Label":"INFORMATIONAL",
        "Normalized":0,
        "Original":"INFORMATIONAL"
      },
      "Title":"1.12 Ensure no root user access key exists",
      "Description":"The root user is the most privileged user in an AWS
account. AWS Access Keys provide programmatic access to a given AWS account. It is
recommended that all access keys associated with the root user be removed.",
      "Remediation":{
        "Recommendation":{

```

```

        "Text": "For information on how to correct this issue, consult the
        AWS Security Hub controls documentation.",
        "Url": "https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
    }
},
    "ProductFields": {
        "StandardsGuideArn": "arn:aws:securityhub::ruleset/cis-aws-
foundations-benchmark/v/1.2.0",
        "StandardsGuideSubscriptionArn": "arn:aws:securityhub:us-
west-2:111122223333:subscription/cis-aws-foundations-benchmark/v/1.2.0",
        "RuleId": "1.12",
        "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
        "RelatedAWSResources:0/name": "securityhub-iam-root-access-key-
check-67cbb1c4",
        "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
        "StandardsControlArn": "arn:aws:securityhub:us-
west-2:111122223333:control/cis-aws-foundations-benchmark/v/1.2.0/1.12",
        "aws/securityhub/ProductName": "Security Hub",
        "aws/securityhub/CompanyName": "AWS",
        "Resources:0/Id": "arn:aws:iam::111122223333:root",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
    },
    "Resources": [
        {
            "Type": "AwsAccount",
            "Id": "AWS:::Account:111122223333",
            "Partition": "aws",
            "Region": "us-west-2"
        }
    ],
    "Compliance": {
        "Status": "PASSED",
        "SecurityControlId": "IAM.4",
        "AssociatedStandards": [
            {
                "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
            }
        ]
    },
    "WorkflowState": "NEW",

```



```

        "Workflow":{
            "Status":"RESOLVED"
        },
        "RecordState":"ACTIVE",
        "FindingProviderFields":{
            "Severity":{
                "Label":"INFORMATIONAL",
                "Original":"INFORMATIONAL"
            },
            "Types":[
                "Software and Configuration Checks/Industry and Regulatory
Standards/CIS AWS Foundations Benchmark"
            ]
        },
        "ProcessedAt":"2023-11-01T14:12:13.436Z"
    }
}
]
}
}

```

Bukti untuk PCI.IAM.1 (PCI DSS)

```

{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
    "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
    "findings":[
      {
        "SchemaVersion":"2018-10-08",
        "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b",
        "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
        "ProductName":"Security Hub",

```

PCI-DSS"

remediation"

west-2:111122223333:subscription/pci-dss/v/3.2.1",

IAM.4/remediation",

check-67cbb1c4",

west-2:111122223333:control/pci-dss/v/3.2.1/PCI.IAM.1",

aws/securityhub/Product Name": "Security Hub",

aws/securityhub/Company Name": "AWS",

```

"CompanyName": "AWS",
"Region": "us-west-2",
"GeneratorId": "pci-dss/v/3.2.1/PCI.IAM.1",
"AwsAccountId": "111122223333",
"Types": [
  "Software and Configuration Checks/Industry and Regulatory Standards/
  ],
"FirstObservedAt": "2020-10-05T19:18:47.788Z",
"LastObservedAt": "2023-11-01T14:12:02.413Z",
"CreatedAt": "2020-10-05T19:18:47.788Z",
"UpdatedAt": "2023-11-01T14:11:53.720Z",
"Severity": {
  "Product": 0,
  "Label": "INFORMATIONAL",
  "Normalized": 0,
  "Original": "INFORMATIONAL"
},
"Title": "PCI.IAM.1 IAM root user access key should not exist",
"Description": "This AWS control checks whether the root user access key
  is available.",
"Remediation": {
  "Recommendation": {
    "Text": "For information on how to correct this issue, consult the
    AWS Security Hub controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/IAM.4/
  }
},
"ProductFields": {
  "StandardsArn": "arn:aws:securityhub::standards/pci-dss/v/3.2.1",
  "StandardsSubscriptionArn": "arn:aws:securityhub:us-
  west-2:111122223333:subscription/pci-dss/v/3.2.1",
  "ControlId": "PCI.IAM.1",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/
  IAM.4/remediation",
  "RelatedAWSResources:0/name": "securityhub-iam-root-access-key-
  check-67cbb1c4",
  "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
  "StandardsControlArn": "arn:aws:securityhub:us-
  west-2:111122223333:control/pci-dss/v/3.2.1/PCI.IAM.1",
  "aws/securityhub/Product Name": "Security Hub",
  "aws/securityhub/Company Name": "AWS",
  "Resources:0/Id": "arn:aws:iam:111122223333:root",

```

```

        "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b"
    },
    "Resources":[
        {
            "Type":"AwsAccount",
            "Id":"AWS:::Account:111122223333",
            "Partition":"aws",
            "Region":"us-west-2"
        }
    ],
    "Compliance":{
        "Status":"PASSED",
        "RelatedRequirements":[
            "PCI DSS 2.1",
            "PCI DSS 2.2",
            "PCI DSS 7.2.1"
        ],
        "SecurityControlId":"IAM.4",
        "AssociatedStandards":[
            {
                "StandardsId":"standards/pci-dss/v/3.2.1"
            }
        ]
    },
    "WorkflowState":"NEW",
    "Workflow":{
        "Status":"RESOLVED"
    },
    "RecordState":"ACTIVE",
    "FindingProviderFields":{
        "Severity":{
            "Label":"INFORMATIONAL",
            "Original":"INFORMATIONAL"
        },
        "Types":[
            "Software and Configuration Checks/Industry and Regulatory
Standards/PCI-DSS"
        ]
    },
    "ProcessedAt":"2023-11-01T14:12:05.950Z"
}
]

```

```
}
}
```

Kontrol CSPM Security Hub yang didukung

Kontrol CSPM Hub Keamanan berikut saat ini didukung oleh Audit Manager. Anda dapat menggunakan salah satu kata kunci ID kontrol khusus standar berikut saat menyiapkan sumber data untuk kontrol kustom.

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
CIS v1.2.0	1.2	IAM.5
CIS v1.2.0	1.3	IAM.8
CIS v1.2.0	1.4	IAM.3
CIS v1.2.0	1.5	IAM.11
CIS v1.2.0	1.6	IAM.12
CIS v1.2.0	1.7	IAM.13
CIS v1.2.0	1.8	IAM.14
CIS v1.2.0	1.9	IAM.15
CIS v1.2.0	1.10	IAM.16
CIS v1.2.0	1.11	IAM.17
CIS v1.2.0	1.12	IAM.4

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
CIS v1.2.0	1.13	IAM.9
CIS v1.2.0	1.14	IAM.6
CIS v1.2.0	1.16	IAM.2
CIS v1.2.0	1.20	IAM.18
CIS v1.2.0	1.22	IAM.1
CIS v1.2.0	2.1	CloudTrail.1
CIS v1.2.0	2.2	CloudTrail.4
CIS v1.2.0	2.3	CloudTrail.6
CIS v1.2.0	2.4	CloudTrail.5
CIS v1.2.0	2.5	Config.1
CIS v1.2.0	2.6	CloudTrail.7
CIS v1.2.0	2.7	CloudTrail.2
CIS v1.2.0	2.8	KMS.4
CIS v1.2.0	2.9	EC2.6
CIS v1.2.0	3.1	CloudWatch.2
CIS v1.2.0	3.2	CloudWatch.3

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
CIS v1.2.0	3.3	CloudWatch.1
CIS v1.2.0	3.4	CloudWatch.4
CIS v1.2.0	3.5	CloudWatch.5
CIS v1.2.0	3.6	CloudWatch.6
CIS v1.2.0	3.7	CloudWatch.7
CIS v1.2.0	3.8	CloudWatch.8
CIS v1.2.0	3.9	CloudWatch.9
CIS v1.2.0	3.10	CloudWatch.10
CIS v1.2.0	3.11	CloudWatch.11
CIS v1.2.0	3.12	CloudWatch.12
CIS v1.2.0	3.13	CloudWatch.13
CIS v1.2.0	3.14	CloudWatch.14
CIS v1.2.0	4.1	EC2.13
CIS v1.2.0	4.2	EC2.14
CIS v1.2.0	4.3	EC2.2
PCI DSS	PCI.AutoScaling.1	AutoScaling.1

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
PCI DSS	PCI.CloudTrail.1	CloudTrail.1
PCI DSS	PCI.CloudTrail.2	CloudTrail.2
PCI DSS	PCI.CloudTrail.3	CloudTrail.3
PCI DSS	PCI.CloudTrail.4	CloudTrail.4
PCI DSS	PCI.CodeBuild.1	CodeBuild.1
PCI DSS	PCI.CodeBuild.2	CodeBuild.2
PCI DSS	PCI.Config.1	Config.1
PCI DSS	PCI.CW.1	CloudWatch.1
PCI DSS	PCI.DMS.1	DMS.1
PCI DSS	PCI.EC2.1	EC2.1
PCI DSS	PCI.EC2.2	EC2.2
PCI DSS	PCI.EC2.3	EC2.3
PCI DSS	PCI.EC2.4	EC2.12
PCI DSS	PCI.EC2.5	EC2.13
PCI DSS	PCI.EC2.6	EC2.6

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
PCI DSS	PCI.ELBv2.1	ELB.1
PCI DSS	PCI.ES.1	ES.1
PCI DSS	PCI.ES.2	ES.2
PCI DSS	PCI.Guard Duty.1	GuardDuty.1
PCI DSS	PCI.IAM.1	IAM.1
PCI DSS	PCI.IAM.2	IAM.2
PCI DSS	PCI.IAM.3	IAM.3
PCI DSS	PCI.IAM.4	IAM.4
PCI DSS	PCI.IAM.5	IAM.9
PCI DSS	PCI.IAM.6	IAM.6
PCI DSS	PCI.IAM.7	PCI.IAM.7
PCI DSS	PCI.IAM.8	PCI.IAM8.
PCI DSS	PCI.KMS.1	PCI.KMS.4
PCI DSS	PCI.Lambda.1	Lambda.1
PCI DSS	PCI.Lambda.2	Lambda.3

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
PCI DSS	PCI.Opensearch.1	Opensearch.1
PCI DSS	PCI.Opensearch.2	Opensearch.2
PCI DSS	PCI.RDS.1	RDS.1
PCI DSS	PCI.RDS.2	RDS.2
PCI DSS	PCI.Redshift.1	Redshift.1
PCI DSS	PCI.S3.1	S3.1
PCI DSS	PCI.S3.2	S3.2
PCI DSS	PCI.S3.3	S3.3
PCI DSS	PCI.S3.4	S3.4
PCI DSS	PCI.S3.5	S3.5
PCI DSS	PCI.S3.6	S3.1
PCI DSS	PCI.SageMaker.1	SageMaker.1
PCI DSS	PCI.SSM.1	SSM.1
PCI DSS	PCI.SSM.2	SSM.2
PCI DSS	PCI.SSM.3	SSM.3

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
AWS Praktik Terbaik Keamanan Dasar	Account.1	Account.1
AWS Praktik Terbaik Keamanan Dasar	Account.2	Account.2
AWS Praktik Terbaik Keamanan Dasar	ACM.1	ACM.1
AWS Praktik Terbaik Keamanan Dasar	ACM.2	ACM.2
AWS Praktik Terbaik Keamanan Dasar	APIGateway.1	APIGateway.1
AWS Praktik Terbaik Keamanan Dasar	APIGateway.2	APIGateway.2
AWS Praktik Terbaik Keamanan Dasar	APIGateway.3	APIGateway.3
AWS Praktik Terbaik Keamanan Dasar	APIGateway.4	APIGateway.4
AWS Praktik Terbaik Keamanan Dasar	APIGateway.5	APIGateway.5
AWS Praktik Terbaik Keamanan Dasar	APIGateway.8	APIGateway.8
AWS Praktik Terbaik Keamanan Dasar	APIGateway.9	APIGateway.9
AWS Praktik Terbaik Keamanan Dasar	AppSync.2	AppSync.2
AWS Praktik Terbaik Keamanan Dasar	AppSync.5	AppSync.5
AWS Praktik Terbaik Keamanan Dasar	Athena.1	Athena.1
AWS Praktik Terbaik Keamanan Dasar	AutoScaling.1	AutoScaling.1
AWS Praktik Terbaik Keamanan Dasar	AutoScaling.2	AutoScaling.2

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
AWS Praktik Terbaik Keamanan Dasar	AutoScaling.3	AutoScaling.3
AWS Praktik Terbaik Keamanan Dasar	AutoScaling.4	AutoScaling.4
AWS Praktik Terbaik Keamanan Dasar	Autoscaling.5	Autoscaling.5
AWS Praktik Terbaik Keamanan Dasar	AutoScaling.6	AutoScaling.6
AWS Praktik Terbaik Keamanan Dasar	AutoScaling.9	AutoScaling.9
AWS Praktik Terbaik Keamanan Dasar	Backup.1	Backup.1
AWS Praktik Terbaik Keamanan Dasar	CloudFormation.1	CloudFormation.1
AWS Praktik Terbaik Keamanan Dasar	CloudFront.1	CloudFront.1
AWS Praktik Terbaik Keamanan Dasar	CloudFront.2	CloudFront.2
AWS Praktik Terbaik Keamanan Dasar	CloudFront.3	CloudFront.3
AWS Praktik Terbaik Keamanan Dasar	CloudFront.4	CloudFront.4
AWS Praktik Terbaik Keamanan Dasar	CloudFront.5	CloudFront.5
AWS Praktik Terbaik Keamanan Dasar	CloudFront.6	CloudFront.6
AWS Praktik Terbaik Keamanan Dasar	CloudFront.7	CloudFront.7
AWS Praktik Terbaik Keamanan Dasar	CloudFront.8	CloudFront.8
AWS Praktik Terbaik Keamanan Dasar	CloudFront.9	CloudFront.9

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
AWS Praktik Terbaik Keamanan Dasar	CloudFront.10	CloudFront.10
AWS Praktik Terbaik Keamanan Dasar	CloudFront.12	CloudFront.12
AWS Praktik Terbaik Keamanan Dasar	CloudFront.13	CloudFront.13
AWS Praktik Terbaik Keamanan Dasar	CloudTrail.1	CloudTrail.1
AWS Praktik Terbaik Keamanan Dasar	CloudTrail.2	CloudTrail.2
AWS Praktik Terbaik Keamanan Dasar	CloudTrail.3	CloudTrail.3
AWS Praktik Terbaik Keamanan Dasar	CloudTrail.4	CloudTrail.4
AWS Praktik Terbaik Keamanan Dasar	CloudTrail.5	CloudTrail.5
AWS Praktik Terbaik Keamanan Dasar	CloudTrail.6	CloudTrail.6
AWS Praktik Terbaik Keamanan Dasar	CloudTrail.7	CloudTrail.7
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.1	CloudWatch.1
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.2	CloudWatch.2
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.3	CloudWatch.3
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.4	CloudWatch.4
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.5	CloudWatch.5
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.6	CloudWatch.6

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.7	CloudWatch.7
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.8	CloudWatch.8
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.9	CloudWatch.9
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.10	CloudWatch.10
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.11	CloudWatch.11
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.12	CloudWatch.12
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.13	CloudWatch.13
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.14	CloudWatch.14
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.15	CloudWatch.15
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.16	CloudWatch.16
AWS Praktik Terbaik Keamanan Dasar	CloudWatch.17	CloudWatch.17
AWS Praktik Terbaik Keamanan Dasar	CodeBuild.1	CodeBuild.1
AWS Praktik Terbaik Keamanan Dasar	CodeBuild.2	CodeBuild.2
AWS Praktik Terbaik Keamanan Dasar	CodeBuild.3	CodeBuild.3
AWS Praktik Terbaik Keamanan Dasar	CodeBuild.4	CodeBuild.4
AWS Praktik Terbaik Keamanan Dasar	CodeBuild.5	CodeBuild.5

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
AWS Praktik Terbaik Keamanan Dasar	Config.1	Config.1
AWS Praktik Terbaik Keamanan Dasar	DMS.1	DMS.1
AWS Praktik Terbaik Keamanan Dasar	DMS.6	DMS.6
AWS Praktik Terbaik Keamanan Dasar	DMS.7	DMS.7
AWS Praktik Terbaik Keamanan Dasar	DMS.8	DMS.8
AWS Praktik Terbaik Keamanan Dasar	DMS.9	DMS.9
AWS Praktik Terbaik Keamanan Dasar	DocumentDB.1	DocumentDB.1
AWS Praktik Terbaik Keamanan Dasar	DocumentDB.2	DocumentDB.2
AWS Praktik Terbaik Keamanan Dasar	DocumentDB.3	DocumentDB.3
AWS Praktik Terbaik Keamanan Dasar	DocumentDB.4	DocumentDB.4
AWS Praktik Terbaik Keamanan Dasar	DocumentDB.5	DocumentDB.5
AWS Praktik Terbaik Keamanan Dasar	DynamoDB.1	DynamoDB.1
AWS Praktik Terbaik Keamanan Dasar	DynamoDB.2	DynamoDB.2
AWS Praktik Terbaik Keamanan Dasar	DynamoDB.3	DynamoDB.3
AWS Praktik Terbaik Keamanan Dasar	DynamoDB.4	DynamoDB.4
AWS Praktik Terbaik Keamanan Dasar	DynamoDB.6	DynamoDB.6

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
AWS Praktik Terbaik Keamanan Dasar	EC2.1	EC2.1
AWS Praktik Terbaik Keamanan Dasar	EC2.2	EC2.2
AWS Praktik Terbaik Keamanan Dasar	EC2.3	EC2.3
AWS Praktik Terbaik Keamanan Dasar	EC2.4	EC2.4
AWS Praktik Terbaik Keamanan Dasar	EC2.6	EC2.6
AWS Praktik Terbaik Keamanan Dasar	EC2.7	EC2.7
AWS Praktik Terbaik Keamanan Dasar	EC2.8	EC2.8
AWS Praktik Terbaik Keamanan Dasar	EC2.9	EC2.9
AWS Praktik Terbaik Keamanan Dasar	EC2.10	EC2.10
AWS Praktik Terbaik Keamanan Dasar	EC2.12	EC2.12
AWS Praktik Terbaik Keamanan Dasar	EC2.13	EC2.13
AWS Praktik Terbaik Keamanan Dasar	EC2.14	EC2.14
AWS Praktik Terbaik Keamanan Dasar	EC2.15	EC2.15
AWS Praktik Terbaik Keamanan Dasar	EC2.16	EC2.16
AWS Praktik Terbaik Keamanan Dasar	EC2.17	EC2.17
AWS Praktik Terbaik Keamanan Dasar	EC2.18	EC2.18

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
AWS Praktik Terbaik Keamanan Dasar	EC2.19	EC2.19
AWS Praktik Terbaik Keamanan Dasar	EC2.20	EC2.20
AWS Praktik Terbaik Keamanan Dasar	EC2.21	EC2.21
AWS Praktik Terbaik Keamanan Dasar	EC2.22	EC2.22
AWS Praktik Terbaik Keamanan Dasar	EC2.23	EC2.23
AWS Praktik Terbaik Keamanan Dasar	EC2.24	EC2.24
AWS Praktik Terbaik Keamanan Dasar	EC2.25	EC2.25
AWS Praktik Terbaik Keamanan Dasar	EC2.28	EC2.28
AWS Praktik Terbaik Keamanan Dasar	EC2.51	EC2.51
AWS Praktik Terbaik Keamanan Dasar	ECR.1	ECR.1
AWS Praktik Terbaik Keamanan Dasar	ECR.2	ECR.2
AWS Praktik Terbaik Keamanan Dasar	ECR.3	ECR.3
AWS Praktik Terbaik Keamanan Dasar	ECS.1	ECS.1
AWS Praktik Terbaik Keamanan Dasar	ECS.2	ECS.2
AWS Praktik Terbaik Keamanan Dasar	ECS.3	ECS.3
AWS Praktik Terbaik Keamanan Dasar	ECS.4	ECS.4

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
AWS Praktik Terbaik Keamanan Dasar	ECS.5	ECS.5
AWS Praktik Terbaik Keamanan Dasar	ECS.8	ECS.8
AWS Praktik Terbaik Keamanan Dasar	ECS.9	ECS.9
AWS Praktik Terbaik Keamanan Dasar	ECS.10	ECS.10
AWS Praktik Terbaik Keamanan Dasar	ECS.12	ECS.12
AWS Praktik Terbaik Keamanan Dasar	EFS.1	EFS.1
AWS Praktik Terbaik Keamanan Dasar	EFS.2	EFS.2
AWS Praktik Terbaik Keamanan Dasar	EFS.3	EFS.3
AWS Praktik Terbaik Keamanan Dasar	EFS.4	EFS.4
AWS Praktik Terbaik Keamanan Dasar	EKS.1	EKS.1
AWS Praktik Terbaik Keamanan Dasar	EKS.2	EKS.2
AWS Praktik Terbaik Keamanan Dasar	EKS.8	EKS.8
AWS Praktik Terbaik Keamanan Dasar	ElastiCache.1	ElastiCache.1
AWS Praktik Terbaik Keamanan Dasar	ElastiCache.2	ElastiCache.2
AWS Praktik Terbaik Keamanan Dasar	ElastiCache.3	ElastiCache.3
AWS Praktik Terbaik Keamanan Dasar	ElastiCache.4	ElastiCache.4

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
AWS Praktik Terbaik Keamanan Dasar	ElastiCache.5	ElastiCache.5
AWS Praktik Terbaik Keamanan Dasar	ElastiCache.6	ElastiCache.6
AWS Praktik Terbaik Keamanan Dasar	ElastiCache.7	ElastiCache.7
AWS Praktik Terbaik Keamanan Dasar	ElasticBeanstalk.1	ElasticBeanstalk.1
AWS Praktik Terbaik Keamanan Dasar	ElasticBeanstalk.2	ElasticBeanstalk.2
AWS Praktik Terbaik Keamanan Dasar	ElasticBeanstalk.3	ElasticBeanstalk.3
AWS Praktik Terbaik Keamanan Dasar	ELB.1	ELB.1
AWS Praktik Terbaik Keamanan Dasar	ELB.2	ELB.2
AWS Praktik Terbaik Keamanan Dasar	ELB.3	ELB.3
AWS Praktik Terbaik Keamanan Dasar	ELB.4	ELB.4
AWS Praktik Terbaik Keamanan Dasar	ELB.5	ELB.5
AWS Praktik Terbaik Keamanan Dasar	ELB.6	ELB.6
AWS Praktik Terbaik Keamanan Dasar	ELB.7	ELB.7
AWS Praktik Terbaik Keamanan Dasar	ELB.8	ELB.8
AWS Praktik Terbaik Keamanan Dasar	ELB.9	ELB.9

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
AWS Praktik Terbaik Keamanan Dasar	ELB.10	ELB.10
AWS Praktik Terbaik Keamanan Dasar	ELB.12	ELB.12
AWS Praktik Terbaik Keamanan Dasar	ELB.13	ELB.13
AWS Praktik Terbaik Keamanan Dasar	ELB.14	ELB.14
AWS Praktik Terbaik Keamanan Dasar	ELB.16	ELB.16
AWS Praktik Terbaik Keamanan Dasar	ELBv2.1	ELB.1
AWS Praktik Terbaik Keamanan Dasar	EMR.1	EMR.1
AWS Praktik Terbaik Keamanan Dasar	EMR.2	EMR.2
AWS Praktik Terbaik Keamanan Dasar	ES.1	ES.1
AWS Praktik Terbaik Keamanan Dasar	ES.2	ES.2
AWS Praktik Terbaik Keamanan Dasar	ES.3	ES.3
AWS Praktik Terbaik Keamanan Dasar	ES.4	ES.4
AWS Praktik Terbaik Keamanan Dasar	ES.5	ES.5
AWS Praktik Terbaik Keamanan Dasar	ES.6	ES.6
AWS Praktik Terbaik Keamanan Dasar	ES.7	ES.7
AWS Praktik Terbaik Keamanan Dasar	ES.8	ES.8

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
AWS Praktik Terbaik Keamanan Dasar	EventBridge.3	EventBridge.3.
AWS Praktik Terbaik Keamanan Dasar	EventBridge.4	EventBridge.4
AWS Praktik Terbaik Keamanan Dasar	FSx.1	FSx.1
AWS Praktik Terbaik Keamanan Dasar	GuardDuty.1	GuardDuty.1
AWS Praktik Terbaik Keamanan Dasar	IAM.1	IAM.1
AWS Praktik Terbaik Keamanan Dasar	IAM.2	IAM.2
AWS Praktik Terbaik Keamanan Dasar	IAM.3	IAM.3
AWS Praktik Terbaik Keamanan Dasar	IAM.4	IAM.4
AWS Praktik Terbaik Keamanan Dasar	IAM.5	IAM.5
AWS Praktik Terbaik Keamanan Dasar	IAM.6	IAM.6
AWS Praktik Terbaik Keamanan Dasar	IAM.7	IAM.7
AWS Praktik Terbaik Keamanan Dasar	IAM.8	IAM.8
AWS Praktik Terbaik Keamanan Dasar	IAM.9	IAM.9
AWS Praktik Terbaik Keamanan Dasar	IAM.10	IAM.10
AWS Praktik Terbaik Keamanan Dasar	IAM.11	IAM.11
AWS Praktik Terbaik Keamanan Dasar	IAM.12	IAM.12

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
AWS Praktik Terbaik Keamanan Dasar	IAM.13	IAM.13
AWS Praktik Terbaik Keamanan Dasar	IAM.14	IAM.14
AWS Praktik Terbaik Keamanan Dasar	IAM.15	IAM.15
AWS Praktik Terbaik Keamanan Dasar	IAM.16	IAM.16
AWS Praktik Terbaik Keamanan Dasar	IAM.17	IAM.17
AWS Praktik Terbaik Keamanan Dasar	IAM.18	IAM.18
AWS Praktik Terbaik Keamanan Dasar	IAM.19	IAM.19
AWS Praktik Terbaik Keamanan Dasar	IAM.21	IAM.21
AWS Praktik Terbaik Keamanan Dasar	IAM.22	IAM.22
AWS Praktik Terbaik Keamanan Dasar	Kinesis.1	Kinesis.1
AWS Praktik Terbaik Keamanan Dasar	KMS.1	KMS.1
AWS Praktik Terbaik Keamanan Dasar	KMS.2	KMS.2
AWS Praktik Terbaik Keamanan Dasar	KMS.3	KMS.3
AWS Praktik Terbaik Keamanan Dasar	KMS.4	KMS.4
AWS Praktik Terbaik Keamanan Dasar	Lambda.1	Lambda.1
AWS Praktik Terbaik Keamanan Dasar	Lambda.2	Lambda.2

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
AWS Praktik Terbaik Keamanan Dasar	Lambda.3	Lambda.3
AWS Praktik Terbaik Keamanan Dasar	Lambda.5	Lambda.5
AWS Praktik Terbaik Keamanan Dasar	Macie.1	Macie.1
AWS Praktik Terbaik Keamanan Dasar	MQ.5	MQ.5
AWS Praktik Terbaik Keamanan Dasar	MQ.6	MQ.6
AWS Praktik Terbaik Keamanan Dasar	MSK.1	MSK.1
AWS Praktik Terbaik Keamanan Dasar	MSK.2	MSK.2
AWS Praktik Terbaik Keamanan Dasar	Neptune.1	Neptune.1
AWS Praktik Terbaik Keamanan Dasar	Neptune.2	Neptune.2
AWS Praktik Terbaik Keamanan Dasar	Neptune.3	Neptune.3
AWS Praktik Terbaik Keamanan Dasar	Neptune.4	Neptune.4
AWS Praktik Terbaik Keamanan Dasar	Neptune.5	Neptune.5
AWS Praktik Terbaik Keamanan Dasar	Neptune.6	Neptune.6
AWS Praktik Terbaik Keamanan Dasar	Neptune.7	Neptune.7
AWS Praktik Terbaik Keamanan Dasar	Neptune.8	Neptune.8
AWS Praktik Terbaik Keamanan Dasar	Neptune.9	Neptune.9

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
AWS Praktik Terbaik Keamanan Dasar	NetworkFirewall.1	NetworkFirewall.1
AWS Praktik Terbaik Keamanan Dasar	NetworkFirewall.2	NetworkFirewall.2
AWS Praktik Terbaik Keamanan Dasar	NetworkFirewall.3	NetworkFirewall.3
AWS Praktik Terbaik Keamanan Dasar	NetworkFirewall.4	NetworkFirewall.4
AWS Praktik Terbaik Keamanan Dasar	NetworkFirewall.5	NetworkFirewall.5
AWS Praktik Terbaik Keamanan Dasar	NetworkFirewall.6	NetworkFirewall.6
AWS Praktik Terbaik Keamanan Dasar	NetworkFirewall.9	NetworkFirewall.9
AWS Praktik Terbaik Keamanan Dasar	Opensearch.1	Opensearch.1
AWS Praktik Terbaik Keamanan Dasar	Opensearch.2	Opensearch.2
AWS Praktik Terbaik Keamanan Dasar	Opensearch.3	Opensearch.3
AWS Praktik Terbaik Keamanan Dasar	Opensearch.4	Opensearch.4
AWS Praktik Terbaik Keamanan Dasar	Opensearch.5	Opensearch.5

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
AWS Praktik Terbaik Keamanan Dasar	Opensearch.6	Opensearch.6
AWS Praktik Terbaik Keamanan Dasar	Opensearch.7	Opensearch.7
AWS Praktik Terbaik Keamanan Dasar	Opensearch.8	Opensearch.8
AWS Praktik Terbaik Keamanan Dasar	Opensearch.10	Opensearch.10
AWS Praktik Terbaik Keamanan Dasar	PCA.1	PCA.1
AWS Praktik Terbaik Keamanan Dasar	RDS.1	RDS.1
AWS Praktik Terbaik Keamanan Dasar	RDS.2	RDS.2
AWS Praktik Terbaik Keamanan Dasar	RDS.3	RDS.3
AWS Praktik Terbaik Keamanan Dasar	RDS.4	RDS.4
AWS Praktik Terbaik Keamanan Dasar	RDS.5	RDS.5
AWS Praktik Terbaik Keamanan Dasar	RDS.6	RDS.6
AWS Praktik Terbaik Keamanan Dasar	RDS.7	RDS.7
AWS Praktik Terbaik Keamanan Dasar	RDS.8	RDS.8
AWS Praktik Terbaik Keamanan Dasar	RDS.9	RDS.9
AWS Praktik Terbaik Keamanan Dasar	RDS.10	RDS.10
AWS Praktik Terbaik Keamanan Dasar	RDS.11	RDS.11

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
AWS Praktik Terbaik Keamanan Dasar	RDS.12	RDS.12
AWS Praktik Terbaik Keamanan Dasar	RDS.13	RDS.13
AWS Praktik Terbaik Keamanan Dasar	RDS.14	RDS.14
AWS Praktik Terbaik Keamanan Dasar	RDS.15	RDS.15
AWS Praktik Terbaik Keamanan Dasar	RDS.16	RDS.16
AWS Praktik Terbaik Keamanan Dasar	RDS.17	RDS.17
AWS Praktik Terbaik Keamanan Dasar	RDS.18	RDS.18
AWS Praktik Terbaik Keamanan Dasar	RDS.19	RDS.19
AWS Praktik Terbaik Keamanan Dasar	RDS.20	RDS.20
AWS Praktik Terbaik Keamanan Dasar	RDS.21	RDS.21
AWS Praktik Terbaik Keamanan Dasar	RDS.22	RDS.22
AWS Praktik Terbaik Keamanan Dasar	RDS.23	RDS.23
AWS Praktik Terbaik Keamanan Dasar	RDS.24	RDS.24
AWS Praktik Terbaik Keamanan Dasar	RDS.25	RDS.25
AWS Praktik Terbaik Keamanan Dasar	RDS.26	RDS.26
AWS Praktik Terbaik Keamanan Dasar	RDS.27	RDS.27

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
AWS Praktik Terbaik Keamanan Dasar	RDS.34	RDS.34
AWS Praktik Terbaik Keamanan Dasar	RDS.35	RDS.35
AWS Praktik Terbaik Keamanan Dasar	Redshift.1	Redshift.1
AWS Praktik Terbaik Keamanan Dasar	Redshift.2	Redshift.2
AWS Praktik Terbaik Keamanan Dasar	Redshift.3	Redshift.3
AWS Praktik Terbaik Keamanan Dasar	Redshift.4	Redshift.4
AWS Praktik Terbaik Keamanan Dasar	Redshift.6	Redshift.6
AWS Praktik Terbaik Keamanan Dasar	Redshift.7	Redshift.7
AWS Praktik Terbaik Keamanan Dasar	Redshift.8	Redshift.8
AWS Praktik Terbaik Keamanan Dasar	Redshift.9	Redshift.9
AWS Praktik Terbaik Keamanan Dasar	Redshift.10	Redshift.10
AWS Praktik Terbaik Keamanan Dasar	Route53.2	Route53.2
AWS Praktik Terbaik Keamanan Dasar	S3.1	S3.1
AWS Praktik Terbaik Keamanan Dasar	S3.2	S3.2
AWS Praktik Terbaik Keamanan Dasar	S3.3	S3.3
AWS Praktik Terbaik Keamanan Dasar	S3.4	S3.4

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
AWS Praktik Terbaik Keamanan Dasar	S3.5	S3.5
AWS Praktik Terbaik Keamanan Dasar	S3.6	S3.6
AWS Praktik Terbaik Keamanan Dasar	S3.7	S3.7
AWS Praktik Terbaik Keamanan Dasar	S3.8	S3.8
AWS Praktik Terbaik Keamanan Dasar	S3.9	S3.9
AWS Praktik Terbaik Keamanan Dasar	S3.11	S3.11
AWS Praktik Terbaik Keamanan Dasar	S3.12	S3.12
AWS Praktik Terbaik Keamanan Dasar	S3.13	S3.13
AWS Praktik Terbaik Keamanan Dasar	S3.14	S3.14
AWS Praktik Terbaik Keamanan Dasar	S3.15	S3.15
AWS Praktik Terbaik Keamanan Dasar	S3.17	S3.17
AWS Praktik Terbaik Keamanan Dasar	S3.19	S3.19
AWS Praktik Terbaik Keamanan Dasar	S3.19	S3.20
AWS Praktik Terbaik Keamanan Dasar	SageMaker.1	SageMaker.1
AWS Praktik Terbaik Keamanan Dasar	SageMaker.2	SageMaker.2
AWS Praktik Terbaik Keamanan Dasar	SageMaker.3	SageMaker.3

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
AWS Praktik Terbaik Keamanan Dasar	SecretsManager.1	SecretsManager.1
AWS Praktik Terbaik Keamanan Dasar	SecretsManager.2	SecretsManager.2
AWS Praktik Terbaik Keamanan Dasar	SecretsManager.3	SecretsManager.3
AWS Praktik Terbaik Keamanan Dasar	SecretsManager.4	SecretsManager.4
AWS Praktik Terbaik Keamanan Dasar	SNS.1	SNS.1
AWS Praktik Terbaik Keamanan Dasar	SNS.2	SNS.2
AWS Praktik Terbaik Keamanan Dasar	SQS.1	SQS.1
AWS Praktik Terbaik Keamanan Dasar	SSM.1	SSM.1
AWS Praktik Terbaik Keamanan Dasar	SSM.2	SSM.2
AWS Praktik Terbaik Keamanan Dasar	SSM.3	SSM.3
AWS Praktik Terbaik Keamanan Dasar	SSM.4	SSM.4
AWS Praktik Terbaik Keamanan Dasar	StepFunctions.1	StepFunctions.1
AWS Praktik Terbaik Keamanan Dasar	WAF.1	WAF.1
AWS Praktik Terbaik Keamanan Dasar	WAF.2	WAF.2

Standar keamanan	Kata kunci yang didukung di Audit Manager (ID kontrol standar di Security Hub CSPM)	Dokumentasi kontrol terkait (ID kontrol keamanan yang sesuai di Security Hub CSPM)
AWS Praktik Terbaik Keamanan Dasar	WAF.3	WAF.3
AWS Praktik Terbaik Keamanan Dasar	WAF.4	WAF.4
AWS Praktik Terbaik Keamanan Dasar	WAF.6	WAF.6
AWS Praktik Terbaik Keamanan Dasar	WAF.7	WAF.7
AWS Praktik Terbaik Keamanan Dasar	WAF.8	WAF.8
AWS Praktik Terbaik Keamanan Dasar	WAF.10	WAF.10
AWS Praktik Terbaik Keamanan Dasar	WAF.11	WAF.11
AWS Praktik Terbaik Keamanan Dasar	WAF.12	WAF.12

Sumber daya tambahan

- Untuk menemukan bantuan dengan masalah pengumpulan bukti untuk jenis sumber data ini, lihat [Penilaian saya tidak mengumpulkan bukti pemeriksaan kepatuhan dari AWS Security Hub CSPM](#).
- Untuk membuat kontrol kustom menggunakan jenis sumber data ini, lihat [Membuat kontrol khusus di AWS Audit Manager](#).
- Untuk membuat kerangka kerja khusus yang menggunakan kontrol kustom Anda, lihat [Membuat kerangka kerja khusus di AWS Audit Manager](#).
- Untuk menambahkan kontrol kustom Anda ke kerangka kustom yang ada, lihat [Mengedit kerangka kerja khusus di AWS Audit Manager](#).

AWS Panggilan API didukung oleh AWS Audit Manager

Anda dapat menggunakan Audit Manager untuk mengambil snapshot AWS lingkungan Anda sebagai bukti audit. Saat membuat atau mengedit kontrol kustom, Anda dapat menentukan satu atau beberapa panggilan AWS API sebagai pemetaan sumber data untuk pengumpulan bukti. Audit Manager kemudian membuat panggilan API ke yang relevan Layanan AWS, dan mengumpulkan snapshot dari detail konfigurasi untuk AWS sumber daya Anda.

Untuk setiap sumber daya yang berada dalam lingkup panggilan API, Audit Manager menangkap snapshot konfigurasi dan mengubahnya menjadi bukti. Ini menghasilkan satu bukti per sumber daya, sebagai lawan dari satu bukti per panggilan API.

Misalnya, jika panggilan `ec2_DescribeRouteTables` API menangkap snapshot konfigurasi dari lima tabel rute, maka Anda akan mendapatkan lima bukti secara total untuk panggilan API tunggal. Setiap bukti adalah snapshot dari konfigurasi tabel rute individu.

Topik

- [Poin kunci](#)
- [Panggilan API yang didukung untuk sumber data kontrol kustom](#)
- [Panggilan API yang digunakan di AWS License Manager kerangka standar](#)
- [Sumber daya tambahan](#)

Poin kunci

Panggilan API berpaginasi

Banyak yang Layanan AWS mengumpulkan dan menyimpan sejumlah besar data. Akibatnya, ketika panggilan `list`, `describe`, atau `get` API mencoba mengembalikan data Anda, bisa ada banyak hasil. Jika jumlah data terlalu besar untuk dikembalikan dalam satu respons, hasilnya dapat dipecah menjadi bagian-bagian yang lebih mudah dikelola melalui penggunaan `pagination`. Ini membagi hasil menjadi “halaman” data, membuat tanggapan lebih mudah ditangani.

Beberapa di antaranya [Panggilan API yang didukung untuk sumber data kontrol kustom](#) dipaginasikan. Ini berarti bahwa mereka mengembalikan hasil `partial` pada awalnya, dan memerlukan permintaan berikutnya untuk mengembalikan seluruh rangkaian hasil. Misalnya, [operasi Amazon RDS](#) `DescribeDBInstances` mengembalikan hingga 100 instans sekaligus, dan permintaan berikutnya diperlukan untuk mengembalikan halaman hasil berikutnya.

Mulai 08 Maret 2023, Audit Manager mendukung panggilan API berpaginasi sebagai sumber data untuk pengumpulan bukti. Sebelumnya, jika panggilan API berpaginasi digunakan sebagai sumber data, hanya sebagian sumber daya Anda yang dikembalikan dalam respons API (hingga 100 hasil). Sekarang, Audit Manager memanggil operasi API berpaginasi beberapa kali, dan mendapatkan setiap halaman hasil sampai semua sumber daya dikembalikan. Untuk setiap sumber daya, Audit Manager kemudian mengambil snapshot konfigurasi dan menyimpannya sebagai bukti. Karena rangkaian lengkap sumber daya Anda sekarang ditangkap dalam respons API, kemungkinan Anda akan melihat peningkatan jumlah bukti yang dikumpulkan setelah 08 Maret 2023.

Audit Manager menangani paginasi panggilan API untuk Anda secara otomatis. Jika Anda membuat kontrol kustom yang menggunakan panggilan API berpaginasi sebagai sumber data, Anda tidak perlu menentukan parameter pagination apa pun.

Panggilan API yang didukung untuk sumber data kontrol kustom

Dalam kontrol kustom Anda, Anda dapat menggunakan salah satu panggilan API berikut sebagai sumber data. Audit Manager kemudian dapat menggunakan panggilan API ini untuk mengumpulkan bukti tentang AWS penggunaan Anda.

Panggilan API yang didukung	Bagaimana Audit Manager menggunakan API ini untuk mengumpulkan bukti
<u>acm_GetAccountConfiguration</u>	Kumpulkan snapshot dari opsi konfigurasi akun yang terkait dengan Anda Akun AWS.
<u>acm_ListCertificates</u>	Ambil daftar ARN sertifikat dan nama domain.
<u>penskalaan_automatis_DescribeAutoScalingGroups</u>	Kumpulkan snapshot tentang grup Penskalaan Otomatis di grup Anda Akun AWS.
<u>cadangan_ListBackupPlans</u>	Ambil daftar semua rencana cadangan aktif di Anda Akun AWS.
<u>batu dasar_GetModelInvocation</u>	Kumpulkan snapshot dari nilai konfigurasi saat ini untuk logging pemanggilan model untuk model di Anda Akun AWS.

Panggilan API yang didukung	Bagaimana Audit Manager menggunakan API ini untuk mengumpulkan bukti
LoggingConfiguration	
cloudfront_ListDistributions	Ambil daftar semua distribusi di Anda Akun AWS.
cloudtrail_DescribeTrails	Kumpulkan snapshot pengaturan untuk satu atau lebih jalur yang terkait dengan Wilayah saat ini untuk Anda Akun AWS.
cloudtrail_ListTrails	Ambil daftar jalur yang ada di Anda Akun AWS.
cloudwatch_DescribeAlarms	Kumpulkan snapshot konfigurasi alarm yang digunakan untuk Anda Akun AWS.
konfigurasi_DescribeConfigRules	Ambil detail tentang AWS Config aturan Anda.
konfigurasi_DescribeDeliveryChannels	Kumpulkan snapshot konfigurasi untuk saluran pengiriman di dalam Anda Akun AWS.
directconnect_DescribeDirectConnectGateways	Ambil daftar semua Direct Connect gateway Anda.
directconnect_DescribeVirtualGateways	Ambil daftar gateway pribadi virtual yang dimiliki oleh Anda Akun AWS.
docdb_DescribeCertificates	Kumpulkan daftar sertifikat untuk Anda Akun AWS.
docdb_DescribeDBClusterParameterGroups	Kumpulkan daftar DBClusterParameterGroup deskripsi untuk Anda Akun AWS.

Panggilan API yang didukung	Bagaimana Audit Manager menggunakan API ini untuk mengumpulkan bukti
docdb_describedblinstances	Kumpulkan informasi tentang instans Amazon DynamoDB yang disediakan untuk Anda. Akun AWS
cloudwatch_DescribeAlarms	Kumpulkan informasi tentang alarm di Anda Akun AWS.
cloudtrail_DescribeTrails	Kumpulkan snapshot pengaturan untuk satu atau lebih jalur yang terkait dengan Anda Akun AWS.
dynamodb_DescribeTable	Kumpulkan snapshot konfigurasi untuk tabel DynamoDB di Anda. Akun AWS Saat Anda menggunakan API ini sebagai sumber data, Anda tidak perlu memberikan nama tabel DynamoDB tertentu. Sebagai gantinya, Audit Manager menggunakan <code>ListTables</code> operasi untuk mencantumkan semua tabel Anda. Untuk setiap tabel yang terdaftar, Audit Manager kemudian melakukan <code>DescribeTable</code> operasi untuk menghasilkan bukti untuk sumber daya tersebut.
dynamodb_ListBackups	Ambil daftar cadangan DynamoDB yang terkait dengan Anda. Akun AWS
dynamodb_ListTables	Ambil daftar semua nama tabel yang terkait dengan titik akhir Anda Akun AWS dan Anda saat ini.
ec2_DescribeAddresses	Kumpulkan snapshot dari alamat IP Elastic Anda.
ec2_DescribeCustomerGateways	Kumpulkan snapshot dari gateway pelanggan VPN Anda.
ec2_DescribeEgressOnlyInternetGateways	Kumpulkan snapshot dari gateway internet khusus pintu masuk Anda.

Panggilan API yang didukung	Bagaimana Audit Manager menggunakan API ini untuk mengumpulkan bukti
ec2_DescribeFlowLogs	Kumpulkan snapshot dari log alur Anda.
ec2_DescribeInstances	Kumpulkan snapshot dari instance Anda.
ec2_DescribeInternetGateways	Kumpulkan snapshot dari gateway internet Anda.
ec2_DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations	Kumpulkan deskripsi asosiasi antara grup antarmuka virtual dan tabel rute gateway lokal di Akun AWS.
ec2_DescribeLocalGateways	Kumpulkan snapshot dari gateway lokal Anda.
ec2_DescribeLocalGatewayVirtualInterfaces	Kumpulkan snapshot dari antarmuka virtual gateway lokal Anda.
ec2_DescribeNatGateways	Kumpulkan snapshot dari gateway NAT Anda.
ec2_DescribeNetworkAcls	Kumpulkan snapshot dari ACL jaringan Anda.
ec2_DescribeRouteTables	Kumpulkan snapshot dari tabel rute Anda.
ec2_DescribeSecurityGroups	Kumpulkan snapshot dari grup keamanan Anda.
ec2_DescribeSecurityGroupRules	Kumpulkan snapshot dari satu atau beberapa aturan grup keamanan Anda.

Panggilan API yang didukung	Bagaimana Audit Manager menggunakan API ini untuk mengumpulkan bukti
ec2_DescribeTransitGateways	Kumpulkan snapshot dari gateway transit Anda.
ec2_DescribeVolumes	Kumpulkan snapshot dari titik akhir VPC Anda.
ec2_DescribeVpcs	Kumpulkan snapshot dari VPC Anda.
ec2_DescribeVpcEndpoints	Kumpulkan snapshot dari titik akhir VPC Anda.
ec2_DescribeVpcEndpointConnections	Kumpulkan snapshot koneksi titik akhir VPC ke layanan titik akhir VPC Anda, termasuk titik akhir yang menunggu penerimaan Anda.
ec2_DescribeVpcEndpointServiceConfigurations	Kumpulkan snapshot konfigurasi layanan titik akhir VPC di Akun AWS.
ec2_DescribeVpcPeeringConnections	Kumpulkan snapshot koneksi VPN Anda.
ec2_DescribeVpnConnections	Kumpulkan snapshot koneksi VPN Anda.
ec2_DescribeVpnGateways	Kumpulkan snapshot dari gateway pribadi virtual Anda.
ec2_GetEbsDefaultKmsKeyId	Kumpulkan snapshot dari default AWS KMS key untuk enkripsi EBS untuk Akun AWS di Wilayah saat ini.
ec2_GetEbsEncryptionByDefault	Jelaskan apakah enkripsi EBS secara default diaktifkan untuk Akun AWS di Wilayah saat ini.

Panggilan API yang didukung	Bagaimana Audit Manager menggunakan API ini untuk mengumpulkan bukti
ecs_DescribeClusters	Kumpulkan snapshot dari cluster ECS Anda.
ex_DescribeAddonVersions	Kumpulkan snapshot dari versi add-on Anda.
Elasticache_DescribeCacheClusters	Kumpulkan snapshot dari cluster yang Anda sediakan.
Elasticache_DescribeServiceUpdates	Kumpulkan snapshot pembaruan layanan untuk Amazon ElastiCache.
elasticfilesystem_DescribeAccessPoints	Kumpulkan snapshot dari titik akses Amazon EFS di situs Anda Akun AWS.
elasticfilesystem_DescribeFileSystems	Kumpulkan snapshot sistem file Amazon EFS Anda.
elasticloadbalancingv2_DescribeLoadBalancers	Kumpulkan snapshot penyeimbang beban di Anda Akun AWS.
ElasticLoadBalancingV2_describesSLPolicies	Kumpulkan snapshot kebijakan yang Anda gunakan untuk negosiasi SSL.
elasticloadbalancingv2_DescribeTargetGroups	Kumpulkan snapshot dari kelompok target ELB Anda.

Panggilan API yang didukung	Bagaimana Audit Manager menggunakan API ini untuk mengumpulkan bukti
elasticmapreduce_ListSecurityConfigurations	Ambil daftar konfigurasi keamanan yang terlihat oleh Anda Akun AWS, bersama dengan tanggal dan waktu pembuatannya, serta namanya.
acara_ListConnections	Ambil daftar EventBridge koneksi Amazon di Anda Akun AWS.
acara_ListEventBuses	Ambil daftar bus EventBridge acara Amazon di Anda Akun AWS, termasuk bus acara default, bus acara khusus, dan bus acara mitra.
acara_ListEventSources	Ambil daftar sumber acara mitra yang telah dibagikan dengan Anda Akun AWS.
acara_ListRules	Ambil daftar EventBridge aturan Amazon Anda.
selang_perapia_ListDeliveryStreams	Ambil daftar aliran pengiriman Anda.
fsx_DescribeFileSystems	Kumpulkan snapshot dari sistem file yang dimiliki oleh Anda Akun AWS.
penjaga_ListDetectors	Ambil daftar sumber daya detectorIds GuardDuty detektor Amazon Anda.
iam_GenerateCredentialReport	Buat laporan kredensi untuk Anda Akun AWS.
iam_GetAccountPasswordPolicy	Kumpulkan snapshot kebijakan kata sandi untuk Anda Akun AWS.
iam_GetAccountSummary	Kumpulkan snapshot penggunaan entitas IAM dan kuota IAM di Anda Akun AWS
iam_ListGroups	Ambil daftar grup IAM yang terkait dengan awalan jalur yang tersedia di Anda Akun AWS.

Panggilan API yang didukung	Bagaimana Audit Manager menggunakan API ini untuk mengumpulkan bukti
iam_ ListOpenIDConnectProviders	Ambil daftar objek sumber daya penyedia IAM OpenID Connect (OIDC) yang didefinisikan di file Anda. Akun AWS
iam_ ListPolicies	Ambil daftar semua kebijakan terkelola yang tersedia di Anda Akun AWS, termasuk kebijakan terkelola yang ditentukan pelanggan Anda sendiri dan semua kebijakan terkelola AWS.
iam_ ListRoles	Ambil daftar peran IAM yang terkait dengan awalan jalur yang tersedia di Anda Akun AWS.
IAM_ ListSamlProviders	Ambil daftar objek sumber daya penyedia SAML yang ditentukan di IAM di Anda. Akun AWS
iam_ ListUsers	Ambil daftar pengguna IAM di Anda Akun AWS.
iam_ ListVirtualMFADevices	Ambil daftar perangkat MFA virtual yang ditentukan di perangkat Anda Akun AWS.
kafka_ ListClusters	Ambil daftar cluster Amazon MSK di Anda Akun AWS.
kafka_ ListKafkaVersions	Ambil daftar objek versi Apache Kafka di Anda Akun AWS.
kinesis_ ListStreams	Ambil daftar aliran data Kinesis Anda.
kms_ GetKeyPolicy	Audit Manager menggunakan API ini untuk mengumpulkan snapshot dari kebijakan utama untuk AWS KMS keys di Anda Akun AWS. Saat Anda menggunakan API ini sebagai sumber data, Anda tidak perlu memberikan nama tertentu AWS KMS key. Sebagai gantinya, Audit Manager menggunakan ListKeys operasi untuk mencantumkan semua kunci KMS Anda. Untuk setiap kunci KMS yang terdaftar, Audit Manager kemudian melakukan GetKeyPolicy operasi untuk menghasilkan bukti untuk sumber daya tersebut.

Panggilan API yang didukung	Bagaimana Audit Manager menggunakan API ini untuk mengumpulkan bukti
<u>kms_ GetKeyRotationStatus</u>	Audit Manager menggunakan API ini untuk mengumpulkan snapshot apakah rotasi otomatis diaktifkan untuk AWS KMS keys di Anda Akun AWS. Saat Anda menggunakan API ini sebagai sumber data, Anda tidak perlu memberikan nama tertentu AWS KMS key. Sebagai gantinya, Audit Manager menggunakan ListKeys operasi untuk mencantumkan semua kunci KMS Anda. Untuk setiap kunci KMS yang terdaftar, Audit Manager kemudian melakukan GetKeyRotationStatus operasi untuk menghasilkan bukti untuk sumber daya tersebut.
<u>kms_ ListKeys</u>	Ambil daftar AWS KMS keys di Anda Akun AWS.
<u>Lambda_ ListFunctions</u>	Ambil daftar fungsi Lambda di Anda Akun AWS, dengan konfigurasi khusus versi masing-masing.
<u>RDS_describeDBClusters</u>	Kumpulkan snapshot dari cluster Amazon Aurora DB dan Multi-AZ cluster DB yang ada di situs Anda Akun AWS.
<u>RDS_describeDBInstances</u>	Kumpulkan snapshot dari instance RDS yang disediakan di Anda. Akun AWS
<u>rds_ DescribeDBInstanceAutomatedBackups</u>	Kumpulkan snapshot dari cadangan untuk instans saat ini dan yang dihapus di Anda Akun AWS.
<u>rds_ DescribeDBSecurityGroups</u>	Kumpulkan snapshot dari DBSecurityGroups dalam Anda Akun AWS.
<u>pergeseran merah_ DescribeClusters</u>	Kumpulkan snapshot dari cluster Amazon Redshift yang disediakan di Anda. Akun AWS

Panggilan API yang didukung	Bagaimana Audit Manager menggunakan API ini untuk mengumpulkan bukti
s3_GetBucketEncryption	Kumpulkan snapshot yang menunjukkan konfigurasi enkripsi default untuk bucket S3 Anda. Saat Anda menggunakan API ini sebagai sumber data, Anda tidak perlu memberikan nama bucket S3 tertentu. Sebagai gantinya, Audit Manager menggunakan <code>ListBuckets</code> operasi untuk membuat daftar bucket yang dibuat Wilayah AWS sama dengan penilaian Anda. Untuk setiap bucket yang terdaftar, Audit Manager kemudian melakukan <code>GetBucketEncryption</code> operasi untuk menghasilkan bukti untuk sumber daya tersebut. Audit Manager hanya dapat memberikan status enkripsi untuk bucket yang dibuat Wilayah AWS sama dengan penilaian Anda. Jika Anda perlu melihat status enkripsi semua bucket S3 Anda di beberapa bucket Wilayah AWS, sebaiknya buat penilaian di masing-masing Wilayah AWS tempat Anda memiliki bucket S3.
s3_ListBuckets	Ambil daftar bucket S3 di Anda Akun AWS. Audit Manager hanya dapat mencantumkan bucket yang dibuat Wilayah AWS sama dengan penilaian Anda. Jika Anda perlu melihat semua bucket S3 Anda di beberapa Wilayah AWS s, sebaiknya buat penilaian di masing-masing Wilayah AWS tempat Anda memiliki bucket S3.
sagemaker_ListAlgorithms	Ambil daftar algoritma pembelajaran mesin di Anda Akun AWS.
sagemaker_ListDomains	Ambil daftar domain di Anda Akun AWS.
sagemaker_ListEndpoints	Ambil daftar titik akhir di Anda Akun AWS.
sagemaker_ListEndpointConfigs	Ambil daftar konfigurasi titik akhir di Anda Akun AWS.

Panggilan API yang didukung	Bagaimana Audit Manager menggunakan API ini untuk mengumpulkan bukti
<u>sagemaker_ ListFlowDefinitions</u>	Ambil daftar definisi alur di Anda Akun AWS.
<u>sagemaker_ ListHumanTaskUis</u>	Ambil daftar antarmuka tugas manusia di Anda Akun AWS.
<u>sagemaker_ ListLabelingJobs</u>	Ambil daftar pekerjaan pelabelan di Anda Akun AWS.
<u>sagemaker_ ListModels</u>	Ambil daftar model di Anda Akun AWS.
<u>sagemaker_ _ListModel BiasJobDefinitions</u>	Ambil daftar definisi pekerjaan bias model di Anda Akun AWS.
<u>sagemaker_ ListModelCards</u>	Ambil daftar kartu model di kartu Anda Akun AWS.
<u>sagemaker_ ListModelQualityJobDefinitions</u>	Ambil daftar definisi pekerjaan pemantauan kualitas model di Anda Akun AWS.
<u>sagemaker_ ListMonitoringAlerts</u>	Ambil daftar peringatan untuk jadwal pemantauan tertentu.
<u>sagemaker_ ListMonitoringSchedules</u>	Ambil daftar semua jadwal pemantauan di Anda Akun AWS.
<u>sagemaker_ ListTrainingJobs</u>	Ambil daftar pekerjaan pelatihan di Anda Akun AWS.
<u>sagemaker_ ListUserProfiles</u>	Ambil daftar profil pengguna di Anda Akun AWS.

Panggilan API yang didukung	Bagaimana Audit Manager menggunakan API ini untuk mengumpulkan bukti
secretmanager_ListSecrets	Ambil daftar rahasia yang disimpan di Anda Akun AWS, tidak termasuk rahasia yang ditandai untuk dihapus.
sns_ListTopics	Ambil daftar topik SNS di Anda Akun AWS.
sqs_ListQueues	Ambil daftar antrian SQS di Anda. Akun AWS
waf-regional_ListWebAcls	Ambil daftar objek WebACLSummary untuk Anda. Akun AWS
waf-regional_ListRules	Ambil daftar RuleSummary objek untuk Anda Akun AWS.
waf_ListRuleGroups	Ambil daftar RuleGroupSummary objek untuk grup aturan di Anda Akun AWS.
waf_ListRules	Ambil daftar RuleSummary objek untuk Anda Akun AWS.
waf_ListWebAcls	Ambil daftar objek WebACLSummary untuk Anda. Akun AWS

Panggilan API yang digunakan di AWS License Manager kerangka standar

Dalam kerangka [AWS License Manager](#) standar, Manajer Audit menggunakan aktivitas khusus yang disebut `GetLicenseManagerSummary` untuk mengumpulkan bukti. Aktivitas ini memanggil tiga API Manajer Lisensi berikut:

- [ListLicenseConfigurations](#)
- [ListAssociationsForLicenseConfiguration](#)
- [ListUsageForLicenseConfiguration](#)

Data yang dikembalikan kemudian diubah menjadi bukti dan dilampirkan ke kontrol yang relevan dalam penilaian Anda.

Contoh

Katakanlah Anda menggunakan dua produk berlisensi (SQL Service 2017 dan Oracle Database Enterprise Edition). Pertama, `GetLicenseManagerSummary` aktivitas memanggil [ListLicenseConfigurations](#) API, yang memberikan rincian konfigurasi lisensi di akun Anda. Selanjutnya, menambahkan data kontekstual tambahan untuk setiap konfigurasi lisensi dengan memanggil [ListUsageForLicenseConfiguration](#) dan [ListAssociationsForLicenseConfiguration](#). Akhirnya, ini mengubah data konfigurasi lisensi menjadi bukti dan melampirkannya ke kontrol masing-masing dalam kerangka kerja (4.5 - Lisensi yang dikelola pelanggan untuk SQL Server 2017 dan 3.0.4 - Lisensi yang dikelola pelanggan untuk Oracle Database Enterprise Edition).

Jika Anda menggunakan produk berlisensi yang tidak tercakup oleh salah satu kontrol dalam kerangka kerja, data konfigurasi lisensi tersebut dilampirkan sebagai bukti ke kontrol berikut: 5.0 - Lisensi yang dikelola pelanggan untuk lisensi lain.

Sumber daya tambahan

- Untuk menemukan bantuan dengan masalah pengumpulan bukti untuk jenis sumber data ini, lihat [Penilaian saya tidak mengumpulkan bukti data konfigurasi untuk AWS Panggilan API](#).
- Untuk membuat kontrol kustom menggunakan jenis sumber data ini, lihat [Membuat kontrol khusus di AWS Audit Manager](#).
- Untuk membuat kerangka kerja khusus yang menggunakan kontrol kustom Anda, lihat [Membuat kerangka kerja khusus di AWS Audit Manager](#).
- Untuk menambahkan kontrol kustom Anda ke kerangka kustom yang ada, lihat [Mengedit kerangka kerja khusus di AWS Audit Manager](#).

AWS CloudTrail nama acara didukung oleh AWS Audit Manager

Anda dapat menggunakan Audit Manager untuk menangkap peristiwa AWS CloudTrail [manajemen](#) dan peristiwa layanan [global](#) sebagai bukti audit. Saat Anda membuat atau mengedit kontrol kustom, Anda dapat menentukan satu atau beberapa nama CloudTrail peristiwa sebagai pemetaan sumber data untuk pengumpulan bukti. Audit Manager kemudian menyaring CloudTrail log Anda berdasarkan kata kunci yang Anda pilih, dan mengimpor hasilnya sebagai bukti aktivitas pengguna.

Note

Audit Manager menangkap peristiwa manajemen dan acara layanan global saja. Peristiwa data dan peristiwa wawasan tidak tersedia sebagai bukti. Untuk informasi selengkapnya

tentang berbagai jenis CloudTrail acara, lihat [CloudTrail konsep](#) di Panduan AWS CloudTrail Pengguna.

Sebagai pengecualian untuk hal di atas, CloudTrail peristiwa berikut tidak didukung oleh Audit Manager:

- kms_ GenerateDataKey
- KMS_Decrypt
- sts_ AssumeRole
- kinesisisvideo_ GetDataEndpoint
- kinesisisvideo_ GetSignalingChannelEndpoint
- kinesisisvideo_ DescribeSignalingChannel
- kinesisisvideo_ DescribeStream

Pada 11 Mei 2023, Manajer Audit tidak lagi mendukung CloudTrail acara read-only sebagai kata kunci untuk pengumpulan bukti. Kami menghapus total 3.135 kata kunci read-only. Karena pelanggan dan Layanan AWS keduanya melakukan panggilan baca ke API, acara read-only berisik. Akibatnya, kata kunci read-only mengumpulkan banyak bukti yang tidak dapat diandalkan atau relevan untuk audit. Read-only kata kunci termasuk ListDescribe,, dan panggilan Get API (misalnya, [GetObject](#) dan [ListBuckets](#) untuk Amazon S3). Jika Anda menggunakan salah satu kata kunci ini untuk pengumpulan bukti, Anda tidak perlu melakukan apa pun. Kata kunci secara otomatis dihapus dari konsol Audit Manager dan dari penilaian Anda, dan bukti tidak lagi dikumpulkan untuk kata kunci ini.

Sumber daya tambahan

- Untuk menemukan bantuan dengan masalah pengumpulan bukti untuk jenis sumber data ini, lihat [Penilaian saya tidak mengumpulkan bukti aktivitas pengguna dari AWS CloudTrail](#).
- Untuk membuat kontrol kustom menggunakan jenis sumber data ini, lihat [Membuat kontrol khusus di AWS Audit Manager](#).
- Untuk membuat kerangka kerja khusus yang menggunakan kontrol kustom Anda, lihat [Membuat kerangka kerja khusus di AWS Audit Manager](#).
- Untuk menambahkan kontrol kustom Anda ke kerangka kustom yang ada, lihat [Mengedit kerangka kerja khusus di AWS Audit Manager](#).

Pengaturan AWS Audit Manager dengan pengaturan yang disarankan

Sebelum mulai menggunakan Audit Manager, penting bagi Anda untuk menyelesaikan tugas persiapan berikut.

Bab ini akan memandu Anda melalui prasyarat, pengaturan akun, izin pengguna, dan langkah-langkah yang diperlukan untuk mengaktifkan dan mengkonfigurasi Audit Manager dengan fitur dan integrasi yang direkomendasikan. Setelah menyelesaikan tugas-tugas ini, Anda akan siap menggunakan Audit Manager dan memulai dengan merampingkan upaya audit dan kepatuhan Anda.

Daftar Isi

- [Prasyarat untuk menyiapkan AWS Audit Manager](#)
 - [Mendaftar untuk Akun AWS](#)
 - [Tambahkan izin yang diperlukan untuk mengakses dan mengaktifkan Audit Manager](#)
 - [Langkah selanjutnya](#)
- [Mengaktifkan AWS Audit Manager](#)
 - [Prasyarat](#)
 - [Prosedur](#)
 - [Langkah selanjutnya](#)
- [Mengaktifkan fitur yang direkomendasikan dan Layanan AWS untuk AWS Audit Manager](#)
 - [Poin kunci](#)
 - [Menyiapkan fitur Audit Manager yang direkomendasikan](#)
 - [Siapkan integrasi yang direkomendasikan dengan yang lain Layanan AWS](#)
 - [Langkah selanjutnya](#)

Prasyarat untuk menyiapkan AWS Audit Manager

Sebelum Anda dapat menggunakan AWS Audit Manager, Anda harus memastikan bahwa Anda telah mengatur izin Anda Akun AWS dan pengguna dengan benar.

Topik

- [Mendaftar untuk Akun AWS](#)
- [Tambahkan izin yang diperlukan untuk mengakses dan mengaktifkan Audit Manager](#)
- [Langkah selanjutnya](#)

Mendaftar untuk Akun AWS

Untuk memulainya AWS, Anda membutuhkan Akun AWS. Untuk informasi tentang membuat Akun AWS, lihat Mem [ulai dengan an Akun AWS](#) di Panduan AWS Account Management Referensi.

Tambahkan izin yang diperlukan untuk mengakses dan mengaktifkan Audit Manager

Anda harus memberi pengguna izin yang diperlukan untuk mengaktifkan Audit Manager. Untuk pengguna yang membutuhkan akses penuh ke Audit Manager, gunakan kebijakan ter [AWSAuditManagerAdministratorAccess](#) kelola. Ini adalah kebijakan AWS terkelola yang tersedia di Anda Akun AWS, dan merupakan kebijakan yang disarankan untuk administrator Audit Manager.

Tip

Sebagai praktik terbaik keamanan, kami sarankan Anda memulai dengan kebijakan terkel AWS ola dan kemudian beralih ke izin dengan hak istimewa terendah. AWS kebijakan terkelola memberikan izin untuk banyak kasus penggunaan umum. Namun, perlu diingat bahwa karena kebijakan ter AWS kelola tersedia untuk digunakan oleh semua AWS pelanggan, kebijakan tersebut mungkin tidak memberikan izin hak istimewa terkecil untuk kasus penggunaan spesifik Anda. Oleh karena itu, kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan [yang dikelola](#) pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, [AWS lihat kebijakan ter](#) kelola di Panduan AWS Identity and Access Management Pengguna.

Untuk memberikan akses dan menambahkan izin bagi pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

Buat rangkaian izin. Ikuti instruksi di [Buat rangkaian izin](#) dalam Panduan Pengguna AWS IAM Identity Center .

- Pengguna yang dikelola di IAM melalui penyedia identitas:

Buat peran untuk federasi identitas. Ikuti instruksi dalam [Buat peran untuk penyedia identitas pihak ketiga \(federasi\)](#) dalam Panduan Pengguna IAM.

- Pengguna IAM:
 - Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam [Buat peran untuk pengguna IAM](#) dalam Panduan Pengguna IAM.
 - (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk dalam [Menambahkan izin ke pengguna \(konsol\)](#) dalam Panduan Pengguna IAM.

Langkah selanjutnya

Sekarang setelah Anda mengatur Akun AWS dan memberikan izin yang diperlukan, Anda siap untuk mengaktifkan Manajer Audit. Untuk instruksi langkah demi langkah, lihat [Mengaktifkan AWS Audit Manager](#).

Mengaktifkan AWS Audit Manager

Sekarang setelah Anda menyelesaikan prasyarat untuk menyiapkan Audit Manager, Anda dapat mengaktifkan layanan di AWS lingkungan Anda.

Di halaman ini Anda akan mempelajari cara mengaktifkan Audit Manager menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API. Pilih metode yang paling sesuai dengan kebutuhan Anda, dan ikuti langkah-langkah yang sesuai untuk mengaktifkan dan menjalankan Audit Manager.

Prasyarat

Pastikan Anda menyelesaikan semua tugas yang dijelaskan di [Prasyarat untuk menyiapkan AWS Audit Manager](#).

Prosedur

Anda dapat mengaktifkan Audit Manager menggunakan Konsol Manajemen AWS, Audit Manager API, atau AWS Command Line Interface (AWS CLI).

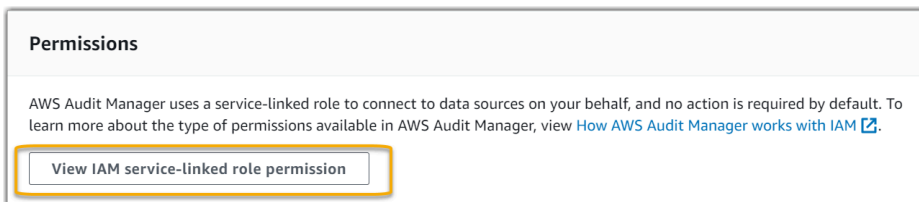
Audit Manager console

Untuk mengaktifkan Audit Manager menggunakan konsol

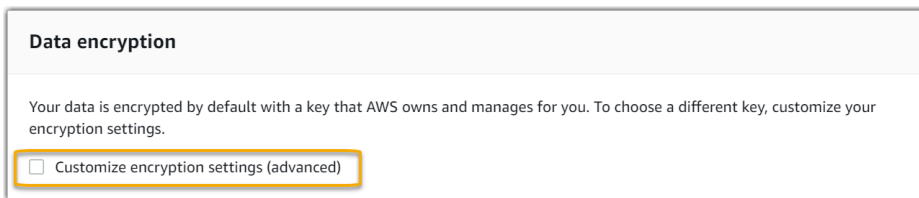
1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Gunakan kredensial identitas IAM Anda untuk masuk.
3. Pilih Siapkan AWS Audit Manager.



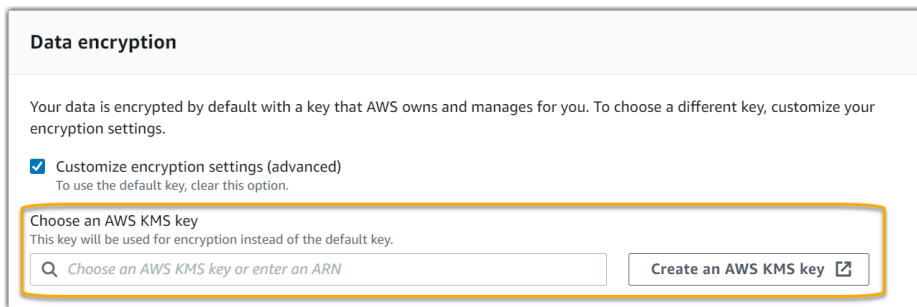
4. Di bawah Izin, tidak ada tindakan yang diperlukan. Ini karena Audit Manager menggunakan peran [terkait layanan](#) untuk terhubung ke sumber data atas nama Anda. Anda dapat meninjau peran terkait layanan dengan memilih Lihat izin peran terkait layanan IAM.



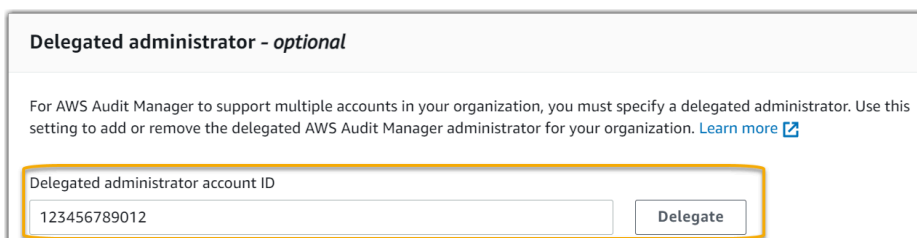
5. Di bawah Enkripsi data, opsi default adalah untuk Manajer Audit untuk membuat dan mengelola AWS KMS key untuk menyimpan data Anda dengan aman.



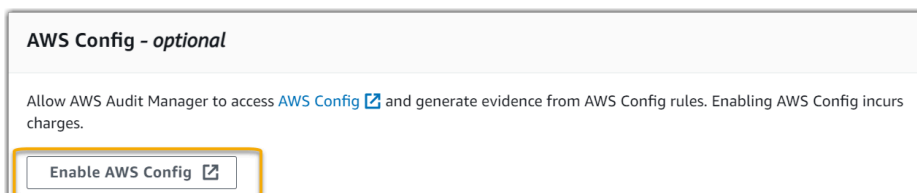
Jika Anda ingin menggunakan kunci yang dikelola pelanggan Anda sendiri untuk mengenkripsi data di Audit Manager, pilih kotak centang di samping Kustomisasi pengaturan enkripsi (lanjutan). Anda kemudian dapat memilih kunci KMS yang ada atau [membuat yang baru](#).



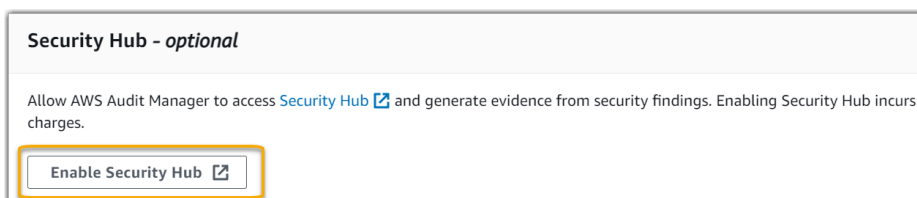
6. (Opsional) Di bawah Administrator yang di delegasikan - opsional, Anda dapat menentukan akun administrator yang didelegasikan jika ingin Audit Manager menjalankan penilaian untuk beberapa akun. Untuk informasi dan rekomendasi lebih lanjut, lihat [Aktifkan dan mengatur AWS Organizations](#).



7. (Opsional) Di bawah AWS Config — opsional, kami sarankan Anda mengaktifkan AWS Config untuk pengalaman yang optimal. Ini memungkinkan Manajer Audit untuk menghasilkan bukti menggunakan AWS Config aturan. Untuk petunjuk dan pengaturan yang disarankan, lihat [Aktifkan dan mengatur AWS Config](#).



8. (Opsional) Di bawah Security Hub CSPM — opsional, kami sarankan Anda mengaktifkan Security Hub CSPM untuk pengalaman yang optimal. Ini memungkinkan Audit Manager untuk menghasilkan bukti menggunakan pemeriksaan CSPM Security Hub. Untuk petunjuk dan pengaturan yang disarankan, lihat [Aktifkan dan mengatur AWS Security Hub CSPM](#).



9. Pilih Pengaturan lengkap untuk menyelesaikan proses penyiapan.



AWS CLI

Untuk mengaktifkan Audit Manager menggunakan AWS CLI

Di baris perintah, jalankan perintah [register-account](#) menggunakan parameter pengaturan berikut:

- `--kms-key`(opsional) — Gunakan parameter ini untuk mengenkripsi data Audit Manager menggunakan kunci yang dikelola pelanggan Anda sendiri. Jika Anda tidak menentukan opsi di sini, Audit Manager membuat dan mengelola AWS KMS key sebuah atas nama Anda untuk penyimpanan data yang aman.
- `--delegated-admin-account`(opsional) — Gunakan parameter ini untuk menetapkan akun administrator yang didelegasikan organisasi Anda untuk Manajer Audit. Jika Anda tidak menentukan opsi di sini, tidak ada administrator yang didelegasikan yang terdaftar.

Contoh masukan (ganti *placeholder text* dengan informasi Anda sendiri):

```
aws auditmanager register-account \  
--kms-key arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \  
--delegated-admin-account 111122224444
```

Contoh keluaran:

```
{  
  "status": "ACTIVE"  
}
```

Untuk informasi selengkapnya tentang AWS CLI dan untuk petunjuk pemasangan AWS CLI alat, lihat berikut ini di Panduan AWS Command Line Interface Pengguna.

- [Panduan Pengguna Antarmuka Baris Perintah AWS](#)
- [Menyiapkan dengan AWS Command Line Interface](#)

Audit Manager API

Untuk mengaktifkan Audit Manager menggunakan API Audit Manager

Gunakan [RegisterAccount](#) operasi dengan parameter pengaturan berikut:

- [KMSKey](#) (opsional) — Gunakan parameter ini untuk mengenkripsi data Audit Manager Anda menggunakan kunci yang dikelola pelanggan Anda sendiri. Jika Anda tidak menentukan opsi di sini, Audit Manager membuat dan mengelola AWS KMS key sebuah atas nama Anda untuk penyimpanan data yang aman.
- [deleg AdminAccount](#) asikan (opsional) — Gunakan parameter ini untuk menentukan akun administrator yang didelegasikan organisasi Anda untuk Manajer Audit. Jika Anda tidak menentukannya, tidak ada administrator yang didelegasikan yang terdaftar.

Contoh masukan (ganti *placeholder text* dengan informasi Anda sendiri):

```
{
  "kmsKey": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
  "delegatedAdminAccount": "111122224444"
}
```

Contoh keluaran:

```
{
  "status": "ACTIVE"
}
```

Langkah selanjutnya

Setelah mengaktifkan Audit Manager, kami sarankan Anda menyiapkan beberapa fitur dan integrasi yang direkomendasikan untuk pengalaman yang optimal. Untuk informasi selengkapnya, lihat [Mengaktifkan fitur yang direkomendasikan dan Layanan AWS untuk AWS Audit Manager](#).

Mengaktifkan fitur yang direkomendasikan dan Layanan AWS untuk AWS Audit Manager

Sekarang setelah Anda mengaktifkan AWS Audit Manager, saatnya untuk mengatur fitur dan integrasi yang direkomendasikan untuk mendapatkan hasil maksimal dari layanan ini.

Poin kunci

Untuk pengalaman optimal di Audit Manager, kami sarankan Anda mengatur fitur-fitur berikut dan mengaktifkan yang berikut ini Layanan AWS.

Tugas

- [Menyiapkan fitur Audit Manager yang direkomendasikan](#)
- [Siapkan integrasi yang direkomendasikan dengan yang lain Layanan AWS](#)
 - [Aktifkan dan mengatur AWS Config](#)
 - [Aktifkan dan mengatur AWS Security Hub CSPM](#)
 - [Aktifkan dan mengatur AWS Organizations](#)

Menyiapkan fitur Audit Manager yang direkomendasikan

Setelah Anda mengaktifkan Audit Manager, sebaiknya aktifkan fitur pencari bukti.

[Pencari bukti](#) menyediakan cara ampuh untuk mencari bukti di Audit Manager. Alih-alih menelusuri folder bukti yang sangat bersarang untuk menemukan apa yang Anda cari, Anda dapat menggunakan pencari bukti untuk menanyakan bukti Anda dengan cepat. Jika Anda menggunakan pencari bukti sebagai administrator yang didelegasikan, Anda dapat mencari bukti di semua akun anggota di organisasi Anda.

Dengan menggunakan kombinasi filter dan pengelompokan, Anda dapat secara progresif mempersempit cakupan permintaan pencarian Anda. Misalnya, jika Anda menginginkan tampilan tingkat tinggi kesehatan sistem Anda, lakukan pencarian luas dan filter berdasarkan penilaian, rentang tanggal, dan kepatuhan sumber daya. Jika tujuan Anda adalah memperbaiki sumber daya tertentu, Anda dapat melakukan pencarian sempit untuk menargetkan bukti untuk kontrol atau ID sumber daya tertentu. Setelah menentukan filter, Anda dapat mengelompokkan dan kemudian melihat pratinjau hasil pencarian yang cocok sebelum membuat laporan penilaian.

Siapkan integrasi yang direkomendasikan dengan yang lain Layanan AWS

Untuk pengalaman optimal di Audit Manager, kami sangat menyarankan Anda mengaktifkan yang berikut ini Layanan AWS:

- **AWS Organizations**— Anda dapat menggunakan Organisasi untuk menjalankan penilaian Manajer Audit di beberapa akun dan mengkonsolidasikan bukti ke dalam akun administrator yang didelegasikan.
- **AWS Security Hub CSPM dan AWS Config** - Manajer Audit mengandalkan ini Layanan AWS sebagai sumber data untuk pengumpulan bukti. Ketika Anda mengaktifkan AWS Config dan Security Hub CSPM, Audit Manager dapat beroperasi dengan fungsionalitas penuhnya, mengumpulkan bukti komprehensif dan secara akurat melaporkan hasil pemeriksaan kepatuhan langsung dari layanan ini.

Important

Jika Anda tidak mengaktifkan dan mengonfigurasi AWS Config dan Security Hub CSPM, Anda tidak akan dapat mengumpulkan bukti yang dimaksudkan untuk banyak kontrol dalam penilaian Manajer Audit Anda. Akibatnya, Anda berisiko mengumpulkan bukti yang tidak lengkap atau gagal untuk kontrol tertentu. Lebih khusus lagi:

- Jika Audit Manager mencoba menggunakan AWS Config sebagai sumber data kontrol, tetapi AWS Config aturan yang diperlukan tidak diaktifkan, tidak ada bukti yang akan dikumpulkan untuk kontrol tersebut.
- Demikian pula, jika Audit Manager mencoba menggunakan Security Hub CSPM sebagai sumber data kontrol, tetapi standar yang diperlukan tidak diaktifkan di Security Hub CSPM, tidak ada bukti yang akan dikumpulkan untuk kontrol tersebut.

Untuk mengurangi risiko ini dan memastikan pengumpulan bukti yang komprehensif, ikuti langkah-langkah di halaman ini untuk mengaktifkan dan mengonfigurasi AWS Config dan Security Hub CSPM sebelum Anda membuat penilaian Manajer Audit Anda.

Aktifkan dan mengatur AWS Config

Banyak kontrol di Audit Manager memerlukan AWS Config sebagai jenis sumber data. Untuk mendukung kontrol ini, Anda harus mengaktifkan AWS Config pada semua akun di setiap akun di Wilayah AWS mana Manajer Audit diaktifkan.

Manajer Audit tidak mengelola AWS Config untuk Anda. Anda dapat mengikuti langkah-langkah ini untuk mengaktifkan AWS Config dan mengkonfigurasi pengaturannya.

 Important

Mengaktifkan AWS Config adalah rekomendasi opsional. Namun, jika Anda mengaktifkan AWS Config, pengaturan berikut diperlukan. Jika Audit Manager mencoba mengumpulkan bukti untuk kontrol yang digunakan AWS Config sebagai jenis sumber data, dan tidak AWS Config diatur seperti yang dijelaskan di bawah ini, tidak ada bukti yang dikumpulkan untuk kontrol tersebut.

Tugas untuk diintegrasikan AWS Config dengan Audit Manager

- [Langkah 1: Aktifkan AWS Config](#)
- [Langkah 2: Konfigurasi AWS Config pengaturan untuk digunakan dengan Audit Manager](#)

Langkah 1: Aktifkan AWS Config

Anda dapat mengaktifkan AWS Config menggunakan AWS Config konsol atau API. Untuk instruksi, lihat [Memulai dengan AWS Config](#) dalam Panduan Developer AWS Config .

Langkah 2: Konfigurasi AWS Config pengaturan untuk digunakan dengan Audit Manager

Setelah Anda mengaktifkan AWS Config, pastikan Anda juga [mengaktifkan AWS Config aturan](#) atau [menerapkan paket kesesuaian](#) untuk standar kepatuhan yang terkait dengan audit Anda. Langkah ini memastikan bahwa Audit Manager dapat mengimpor temuan untuk AWS Config aturan yang Anda aktifkan.

Setelah Anda mengaktifkan AWS Config aturan, sebaiknya tinjau parameter aturan tersebut. Anda kemudian harus memvalidasi parameter tersebut terhadap persyaratan kerangka kepatuhan yang Anda pilih. Jika diperlukan, Anda dapat [memperbarui parameter aturan AWS Config](#) untuk memastikannya selaras dengan persyaratan kerangka kerja. Ini akan membantu memastikan bahwa penilaian Anda mengumpulkan bukti pemeriksaan kepatuhan yang benar untuk kerangka kerja tertentu.

Misalnya, Anda membuat penilaian untuk CIS v1.2.0. Kerangka kerja ini memiliki kontrol bernama [1.4 - Pastikan kunci akses diputar setiap 90 hari atau kurang](#). Di AWS Config, [aturan](#) access-keys- memiliki maxAccessKeyAge parameter dengan nilai default 90 hari. Akibatnya, aturan selaras dengan persyaratan kontrol. Jika Anda tidak menggunakan nilai default, pastikan nilai yang Anda gunakan sama dengan atau lebih besar dari persyaratan 90 hari dari CIS v1.2.0.

Anda dapat menemukan detail parameter default untuk setiap aturan terkelola dalam [AWS Config dokumentasi](#). Untuk petunjuk tentang cara mengonfigurasi aturan, lihat [Bekerja dengan Aturan AWS Config Terkelola](#).

Aktifkan dan mengatur AWS Security Hub CSPM

Banyak kontrol di Audit Manager memerlukan Security Hub CSPM sebagai tipe sumber data. Untuk mendukung kontrol ini, Anda harus mengaktifkan Security Hub CSPM di semua akun di setiap Wilayah tempat Audit Manager diaktifkan.

Audit Manager tidak mengelola Security Hub CSPM untuk Anda. Anda dapat mengikuti langkah-langkah ini untuk mengaktifkan Security Hub CSPM dan mengonfigurasi pengaturannya.

Important

Mengaktifkan Security Hub CSPM adalah rekomendasi opsional. Namun, jika Anda mengaktifkan Security Hub CSPM, pengaturan berikut diperlukan. Jika Audit Manager mencoba mengumpulkan bukti untuk kontrol yang menggunakan Security Hub CSPM sebagai tipe sumber data, dan Security Hub CSPM tidak diatur seperti yang dijelaskan di bawah ini, tidak ada bukti yang dikumpulkan untuk kontrol tersebut.

Tugas untuk diintegrasikan AWS Security Hub CSPM dengan Audit Manager

- [Langkah 1: Aktifkan AWS Security Hub CSPM](#)
- [Langkah 2: Konfigurasi setelan CSPM Security Hub Anda untuk digunakan dengan Audit Manager](#)
- [Langkah 3: Konfigurasi pengaturan Organisasi untuk organisasi Anda](#)

Langkah 1: Aktifkan AWS Security Hub CSPM

Anda dapat mengaktifkan Security Hub CSPM menggunakan konsol atau API. Untuk petunjuk, lihat [Menyiapkan AWS Security Hub CSPM](#) apkan di Panduan AWS Security Hub CSPM Pengguna.

Langkah 2: Konfigurasi setelan CSPM Security Hub Anda untuk digunakan dengan Audit Manager

Setelah Anda mengaktifkan Security Hub CSPM, pastikan Anda juga melakukan hal berikut:

- [Mengaktifkan AWS Config dan mengonfigurasi perekaman sumber daya](#) — Security Hub CSPM menggunakan AWS Config aturan terkait layanan untuk melakukan sebagian besar pemeriksaan keamanan untuk kontrol. Untuk mendukung kontrol ini, AWS Config harus diaktifkan dan dikonfigurasi untuk merekam sumber daya yang diperlukan untuk kontrol yang telah Anda aktifkan di setiap standar yang diaktifkan.
- [Aktifkan semua standar keamanan](#) — Langkah ini memastikan bahwa Audit Manager dapat mengimpor temuan untuk semua standar kepatuhan yang didukung.
- [Aktifkan setelan temuan kontrol konsolidasi di Security Hub CSPM](#) - Pengaturan ini diaktifkan secara default jika Anda mengaktifkan Security Hub CSPM pada atau setelah 23 Februari 2023.

 Note

Saat Anda mengaktifkan temuan konsolidasi, Security Hub CSPM menghasilkan satu temuan untuk setiap pemeriksaan keamanan (bahkan ketika pemeriksaan yang sama digunakan di beberapa standar). Setiap temuan Security Hub CSPM dikumpulkan sebagai satu penilaian sumber daya unik di Audit Manager. Akibatnya, temuan konsolidasi menghasilkan penurunan total penilaian sumber daya unik yang dilakukan Audit Manager untuk temuan Security Hub CSPM. Untuk alasan ini, menggunakan temuan konsolidasi seringkali dapat mengakibatkan pengurangan biaya penggunaan Manajer Audit Anda. Untuk informasi selengkapnya tentang menggunakan Security Hub CSPM sebagai jenis sumber data, lihat [AWS Security Hub CSPM kontrol didukung oleh AWS Audit Manager](#). Untuk informasi selengkapnya tentang harga Audit Manager, lihat [AWS Audit Manager Harga](#).

Langkah 3: Konfigurasi pengaturan Organisasi untuk organisasi Anda

Jika Anda menggunakan AWS Organizations dan ingin mengumpulkan bukti CSPM Security Hub dari akun anggota Anda, Anda juga harus melakukan langkah-langkah berikut di Security Hub CSPM.

Untuk mengatur setelan CSPM Security Hub organisasi Anda

1. Masuk ke Konsol Manajemen AWS dan buka AWS Security Hub CSPM konsol di <https://console.aws.amazon.com/securityhub/>.
2. Menggunakan akun AWS Organizations manajemen Anda, tentukan akun sebagai administrator yang didelegasikan untuk Security Hub CSPM. Untuk informasi selengkapnya, [lihat Menunjuk akun administrator CSPM Hub Keamanan](#) di Panduan Pengguna. AWS Security Hub CSPM

 Note

Pastikan bahwa akun administrator yang didelegasikan yang Anda tetapkan di Security Hub CSPM sama dengan yang Anda gunakan di Audit Manager.

3. Menggunakan akun administrator yang didelegasikan Organisasi Anda, buka Pengaturan, Akun, pilih semua akun, lalu tambahkan mereka sebagai anggota dengan memilih Auto-enroll. Untuk informasi selengkapnya, lihat Meng [aktifkan akun anggota dari organisasi Anda](#) di Panduan AWS Security Hub CSPM Pengguna.
4. Aktifkan konfigurasi untuk setiap akun anggota organisasi. Untuk informasi selengkapnya, lihat Meng [aktifkan akun anggota dari organisasi Anda](#) di Panduan AWS Security Hub CSPM Pengguna.
5. Aktifkan standar keamanan PCI DSS untuk setiap akun anggota organisasi. Standar AWS CIS Foundations Benchmark dan standar AWS Praktik Terbaik Dasar sudah diaktifkan secara default. Untuk informasi selengkapnya, lihat Meng [aktifkan standar keamanan](#) di Panduan AWS Security Hub CSPM Pengguna.

Aktifkan dan mengatur AWS Organizations

Audit Manager mendukung beberapa akun melalui integrasi dengan AWS Organizations. Audit Manager dapat menjalankan penilaian pada beberapa akun dan mengkonsolidasikan bukti ke dalam akun administrator yang didelegasikan. Administrator yang didelegasikan memiliki izin untuk membuat dan mengelola sumber daya Manajer Audit dengan organisasi sebagai zona kepercayaan. Hanya akun manajemen yang dapat menunjuk administrator yang didelegasikan.

 Important

Mengaktifkan AWS Organizations adalah rekomendasi opsional. Namun, jika Anda mengaktifkan AWS Organizations, pengaturan berikut diperlukan.

Tugas untuk diintegrasikan AWS Organizations dengan Audit Manager

- [Langkah 1: Membuat atau bergabung dengan organisasi](#)
- [Langkah 2: Aktifkan semua fitur di organisasi Anda](#)
- [Langkah 3: Tentukan administrator yang didelegasikan untuk Manajer Audit](#)

Langkah 1: Membuat atau bergabung dengan organisasi

Jika Anda Akun AWS bukan bagian dari organisasi, Anda dapat membuat atau bergabung dengan organisasi. Untuk petunjuk, lihat [Membuat dan mengelola organisasi](#) di Panduan AWS Organizations Pengguna.

Langkah 2: Aktifkan semua fitur di organisasi Anda

Selanjutnya, Anda harus mengaktifkan semua fitur di organisasi Anda. Untuk petunjuk, lihat [Mengaktifkan semua fitur di organisasi Anda](#) di Panduan AWS Organizations Pengguna.

Langkah 3: Tentukan administrator yang didelegasikan untuk Manajer Audit

Sebaiknya aktifkan Audit Manager menggunakan akun manajemen Organisasi, lalu tentukan administrator yang didelegasikan. Setelah itu, Anda dapat menggunakan akun administrator yang didelegasikan untuk masuk dan menjalankan penilaian. Sebagai praktik terbaik, sebaiknya buat penilaian hanya menggunakan akun administrator yang didelegasikan, bukan akun manajemen.

Untuk menambah atau mengubah administrator yang didelegasikan setelah Anda mengaktifkan Audit Manager, lihat [Menambahkan administrator yang didelegasikan](#) dan [Mengubah administrator yang didelegasikan](#).

Langkah selanjutnya

Sekarang setelah Anda mengatur Audit Manager dengan pengaturan yang disarankan, Anda siap untuk memulai menggunakan layanan ini.

- Untuk memulai penilaian pertama Anda, lihat [Tutorial untuk Pemilik Audit: Membuat penilaian](#).
- Untuk memperbarui pengaturan Anda di masa mendatang, lihat [Meninjau dan mengonfigurasi Anda AWS Audit Manager pengaturan](#).

Memulai dengan AWS Audit Manager

Gunakan tutorial langkah demi langkah di bagian ini untuk mempelajari cara melakukan tugas menggunakan AWS Audit Manager.

Tip

Tutorial berikut dikategorikan berdasarkan audiens. Pilih tutorial yang sesuai untuk Anda berdasarkan peran Anda sebagai pemilik atau delegasi audit.

- **Pemilik audit** adalah pengguna Audit Manager yang bertanggung jawab untuk membuat dan mengelola penilaian. Dalam dunia bisnis, pemilik audit biasanya profesional tata kelola, manajemen risiko, dan kepatuhan (GRC). Namun, dalam konteks Manajer Audit, individu dari SecOps atau DevOps tim mungkin juga menganggap persona pengguna dari pemilik audit. Pemilik audit dapat meminta bantuan dari ahli materi pokok bahasa—juga dikenal sebagai delegasi—untuk meninjau kontrol tertentu dan memvalidasi bukti. Pemilik audit harus memiliki izin yang diperlukan untuk mengelola penilaian.
- **Delegasi** adalah ahli materi pelajaran dengan keahlian teknis atau bisnis khusus. Meskipun mereka tidak memiliki atau mengelola penilaian Manajer Audit, mereka masih dapat berkontribusi pada penilaian tersebut. Delegasi membantu pemilik audit dengan tugas-tugas seperti memvalidasi bukti untuk kontrol yang termasuk dalam bidang keahlian mereka. Delegasi memiliki izin terbatas di Audit Manager. Ini karena pemilik audit mendelegasikan kumpulan kontrol tertentu untuk ditinjau, dan bukan seluruh penilaian.

Untuk informasi lebih lanjut tentang persona ini dan konsep Manajer Audit lainnya, lihat [audit owner](#) dan [delegate](#) di [Memahami AWS Audit Manager konsep dan terminologi](#) bagian panduan ini.

Untuk informasi selengkapnya tentang izin IAM yang direkomendasikan untuk setiap persona, lihat [Kebijakan yang disarankan untuk persona pengguna di AWS Audit Manager](#)

Tutorial Manajer Audit

[Membuat penilaian](#)

Audiens: Pemilik audit

Ikhtisar: Ikuti petunjuk langkah demi langkah untuk membuat penilaian pertama Anda dan mulai berjalan dengan cepat. Tutorial ini memandu Anda melalui bagaimana Anda dapat menggunakan kerangka kerja standar untuk membuat penilaian dan memulai pengumpulan bukti otomatis.

Meninjau kumpulan kontrol

Penonton: Delegasi

Ringkasan: Membantu pemilik audit dengan meninjau bukti untuk kontrol yang termasuk dalam bidang keahlian Anda. Pelajari cara meninjau kumpulan kontrol dan bukti terkaitnya, menambahkan komentar, mengunggah bukti, dan memperbarui status kontrol.

Tutorial untuk Pemilik Audit: Membuat penilaian

Tutorial ini memberikan pengantar untuk AWS Audit Manager. Dalam tutorial ini, Anda membuat penilaian menggunakan [AWS Audit Manager Contoh Kerangka](#). Dengan membuat penilaian, Anda memulai proses pengumpulan bukti otomatis yang sedang berlangsung untuk kontrol dalam kerangka itu.

Note

AWS Audit Manager membantu mengumpulkan bukti yang relevan untuk memverifikasi kepatuhan terhadap kerangka kerja dan peraturan kepatuhan tertentu. Namun, itu tidak menilai kepatuhan Anda sendiri. Bukti yang dikumpulkan oleh AWS Audit Manager karena itu mungkin tidak mencakup semua informasi tentang AWS penggunaan Anda yang diperlukan untuk audit. AWS Audit Manager bukan pengganti penasihat hukum atau pakar kepatuhan.

Prasyarat

Sebelum memulai tutorial ini, pastikan Anda memenuhi persyaratan berikut:

- Anda menyelesaikan semua prasyarat yang dijelaskan di [Pengaturan AWS Audit Manager dengan pengaturan yang disarankan](#). Anda harus menggunakan Akun AWS dan AWS Audit Manager konsol untuk menyelesaikan tutorial ini.
- Identitas IAM Anda diberikan dengan izin yang sesuai untuk membuat dan mengelola penilaian di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [Izinkan](#)

[pengguna akses administrator penuh ke AWS Audit Manager](#) dan [izinkan akses manajemen pengguna ke AWS Audit Manager](#).

- Anda terbiasa dengan terminologi dan fungsionalitas Audit Manager. Untuk gambaran umum, lihat [Apa itu AWS Audit Manager?](#) dan [Memahami AWS Audit Manager konsep dan terminologi](#).

Prosedur

Tugas

- [Langkah 1: Tentukan detail penilaian](#)
- [Langkah 2: Tentukan Akun AWS dalam ruang lingkup](#)
- [Langkah 3: Tentukan pemilik audit](#)
- [Langkah 4: Tinjau dan buat](#)

Langkah 1: Tentukan detail penilaian

Untuk langkah pertama, pilih kerangka kerja dan berikan informasi dasar untuk penilaian Anda.

Untuk menentukan detail penilaian

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Pilih Luncurkan AWS Audit Manager.
3. Di spanduk hijau di bagian atas layar, pilih Mulai dengan kerangka kerja.
4. Pilih kerangka kerja yang Anda inginkan, lalu pilih Buat penilaian dari kerangka kerja. Untuk tutorial ini, gunakan Kerangka AWS Audit Manager Sampel.
5. Di bawah Nama Penilaian, masukkan nama untuk penilaian Anda.
6. (Opsional) Di bawah Deskripsi penilaian, masukkan deskripsi untuk penilaian Anda.
7. Di bawah Tujuan laporan penilaian, pilih bucket S3 tempat Anda ingin menyimpan laporan penilaian Anda.
8. Di bawah Frame works, konfirmas AWS Audit Manager akan bahwa Kerangka Sampel dipilih.
9. (Opsional) Di bawah Tag, pilih Tambahkan tag baru untuk mengaitkan tag dengan penilaian Anda. Anda dapat menentukan kunci dan nilai untuk setiap tag. Kunci tag adalah wajib dan dapat digunakan sebagai kriteria pencarian saat Anda mencari penilaian ini.
10. Pilih Berikutnya.

Langkah 2: Tentukan Akun AWS dalam ruang lingkup

Selanjutnya, tentukan AWS akun yang ingin Anda sertakan dalam lingkup penilaian Anda.

AWS Audit Manager terintegrasi dengan AWS Organizations, sehingga Anda dapat menjalankan penilaian Manajer Audit di beberapa akun dan mengkonsolidasikan bukti ke dalam akun administrator yang didelegasikan. Untuk mengaktifkan Organisasi di Audit Manager (jika Anda belum melakukannya), lihat [Aktifkan dan mengatur AWS Organizations](#) di halaman Pengaturan panduan ini.

Note

Audit Manager dapat mendukung hingga 200 akun dalam lingkup penilaian. Jika Anda mencoba memasukkan lebih dari 200 akun, pembuatan penilaian akan gagal. Selain itu, jika Anda mencoba menambahkan lebih dari 250 akun unik di semua penilaian Anda, pembuatan penilaian akan gagal.

Untuk menentukan akun dalam cakupan

1. Di bawah Akun AWS, pilih Akun AWS yang ingin Anda sertakan dalam lingkup penilaian Anda.
 - Jika Anda mengaktifkan Organisasi di Audit Manager, beberapa akun akan terdaftar.
 - Jika Anda tidak mengaktifkan Organisasi di Audit Manager, hanya akun Anda saat ini yang terdaftar.
2. Pilih Berikutnya.

Langkah 3: Tentukan pemilik audit

Pada langkah ini, Anda menentukan pemilik audit untuk penilaian Anda. Pemilik audit adalah individu di tempat kerja Anda—biasanya dari GRC, SecOps, atau DevOps tim—yang bertanggung jawab untuk mengelola penilaian Manajer Audit. Kami menyarankan agar mereka menggunakan [AWSAuditManagerAdministratorAccess](#) kebijakan tersebut.

Untuk menentukan pemilik audit

1. Di bawah Pemilik audit, pilih pemilik audit untuk penilaian Anda. Untuk menemukan pemilik audit tambahan, gunakan bilah pencarian untuk mencari berdasarkan nama atau Akun AWS.
2. Pilih Berikutnya.

Langkah 4: Tinjau dan buat

Tinjau informasi untuk penilaian Anda. Untuk mengubah informasi untuk satu langkah, pilih **Edit**. Setelah selesai, pilih **Buat penilaian** untuk memulai pengumpulan bukti yang sedang berlangsung.

Setelah Anda membuat penilaian, pengumpulan bukti berlanjut hingga Anda [mengubah status penilaian](#) menjadi tidak aktif. Atau, Anda dapat menghentikan pengumpulan bukti untuk kontrol tertentu dengan [mengubah status kontrol](#) menjadi tidak aktif.

Note

Bukti otomatis tersedia 24 jam setelah Anda membuat penilaian. Audit Manager secara otomatis mengumpulkan bukti dari berbagai sumber data, dan frekuensi pengumpulan bukti tersebut didasarkan pada jenis bukti. Untuk informasi selengkapnya, lihat [Frekuensi pengumpulan bukti](#) dalam panduan ini.

Sumber daya tambahan

Kami menyarankan Anda untuk terus mempelajari lebih lanjut tentang konsep dan alat yang diperkenalkan dalam tutorial ini. Anda dapat melakukannya dengan meninjau sumber daya berikut:

- [Meninjau detail penilaian di AWS Audit Manager](#)— Memperkenalkan Anda ke halaman detail penilaian di mana Anda dapat menjelajahi berbagai komponen penilaian Anda.
- [Mengelola penilaian di AWS Audit Manager](#)- Dibangun di atas tutorial ini dan memberikan informasi mendalam tentang konsep dan tugas untuk mengelola penilaian. Dalam bagian ini, kami sangat menyarankan Anda memeriksa topik-topik berikut:
 - Cara [membuat penilaian](#) dari kerangka kerja yang berbeda
 - Cara [meninjau bukti dalam penilaian](#) dan [menghasilkan laporan penilaian](#)
 - Cara [mengubah status penilaian](#) atau [menghapus penilaian](#)
- [Menggunakan pustaka kerangka kerja untuk mengelola kerangka kerja di AWS Audit Manager](#)- Memperkenalkan pustaka kerangka kerja dan menjelaskan cara [membuat kerangka kerja khusus](#) untuk kebutuhan kepatuhan spesifik Anda sendiri.
- [Menggunakan pustaka kontrol untuk mengelola kontrol di AWS Audit Manager](#)- Memperkenalkan pustaka kontrol dan menjelaskan cara [membuat kontrol khusus](#) untuk digunakan dalam kerangka kerja kustom Anda.

- [Memahami AWS Audit Manager konsep dan terminologi](#)— Menyediakan definisi untuk konsep dan terminologi yang digunakan dalam Audit Manager.
- [Video] [Kumpulkan Bukti dan Kelola Data Audit Menggunakan AWS Audit Manager](#) — Menunjukkan proses pembuatan penilaian yang dijelaskan dalam tutorial ini, dan tugas-tugas lain seperti meninjau kontrol dan membuat laporan penilaian.

Tutorial untuk Delegasi: Meninjau kumpulan kontrol

Tutorial ini menjelaskan cara meninjau kumpulan kontrol yang dibagikan dengan Anda oleh pemilik audit di AWS Audit Manager.

Pemilik audit menggunakan Audit Manager untuk membuat penilaian dan mengumpulkan bukti untuk kontrol dalam penilaian tersebut. Terkadang pemilik audit mungkin memiliki pertanyaan atau membutuhkan bantuan saat memvalidasi bukti untuk kumpulan kontrol. Dalam situasi ini, pemilik audit dapat mendelegasikan kumpulan kontrol ke ahli materi pelajaran untuk ditinjau.

Sebagai delegasi, Anda membantu pemilik audit untuk meninjau bukti yang dikumpulkan untuk kontrol yang termasuk dalam bidang keahlian Anda.

Prasyarat

Sebelum Anda memulai tutorial ini, pastikan bahwa Anda terlebih dahulu memenuhi persyaratan berikut:

- Anda Akun AWS sudah diatur. Untuk menyelesaikan tutorial ini, Anda harus menggunakan konsol Audit Manager Akun AWS dan Anda. Untuk informasi selengkapnya, lihat [Pengaturan AWS Audit Manager dengan pengaturan yang disarankan](#).
- Anda terbiasa dengan terminologi dan fungsionalitas Audit Manager. Untuk gambaran umum Manajer Audit, lihat [Apa itu AWS Audit Manager?](#) dan [Memahami AWS Audit Manager konsep dan terminologi](#).

Prosedur

Tugas

- [Langkah 1: Tinjau notifikasi](#)

- [Langkah 2: Tinjau kumpulan kontrol dan bukti terkait](#)
- [Langkah 3. Tambahkan bukti manual \(opsional\)](#)
- [Langkah 4. Menambahkan komentar untuk kontrol \(opsional\)](#)
- [Langkah 5: Tandai kontrol sebagai ditinjau \(opsional\)](#)
- [Langkah 6. Kirim kembali set kontrol yang ditinjau ke pemilik audit](#)

Langkah 1: Tinjau notifikasi

Mulailah dengan masuk ke Audit Manager tempat Anda dapat mengakses notifikasi untuk melihat kumpulan kontrol yang telah didelegasikan kepada Anda untuk ditinjau.

Untuk meninjau notifikasi Anda

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi kiri, pilih Pemberitahuan.
3. Pada halaman Notifikasi, Anda meninjau daftar kumpulan kontrol yang telah didelegasikan kepada Anda. Tabel notifikasi mencakup informasi berikut:

Nama	Deskripsi
Tanggal	Tanggal ketika set kontrol didelegasikan.
Penilaian	Nama penilaian yang terkait dengan kumpulan kontrol. Anda dapat memilih nama penilaian untuk membuka halaman detail penilaian.
Set kontrol	Nama kumpulan kontrol yang didelegasikan kepada Anda untuk ditinjau.
Sumber	Pengguna atau peran yang mendelegasikan set kontrol kepada Anda.
Deskripsi	Instruksi peninjauan yang diberikan oleh pemilik audit.

 Tip

Anda juga dapat berlangganan topik SNS untuk menerima peringatan email saat kumpulan kontrol ditugaskan kepada Anda untuk ditinjau. Untuk informasi selengkapnya, lihat [Pemberitahuan di AWS Audit Manager](#).

Langkah 2: Tinjau kumpulan kontrol dan bukti terkait

Langkah selanjutnya adalah meninjau kumpulan kontrol yang didelegasikan oleh pemilik audit kepada Anda. Dengan memeriksa kontrol dan buktinya, Anda dapat menentukan apakah ada tindakan tambahan yang diperlukan untuk kontrol. Tindakan tambahan dapat mencakup mengunggah bukti tambahan secara manual untuk menunjukkan kepatuhan, atau meninggalkan komentar tentang kontrol tersebut.

Untuk meninjau kumpulan kontrol

1. Dari halaman Notifikasi, tinjau daftar kumpulan kontrol yang didelegasikan kepada Anda. Kemudian identifikasi mana yang ingin Anda tinjau dan pilih nama penilaian terkait.
2. Di bawah tab Kontrol pada halaman detail penilaian, gulir ke bawah ke tabel Kumpulan kontrol.
3. Di bawah kolom Kontrol dikelompokkan berdasarkan kumpulan kontrol, perluas nama kumpulan kontrol untuk menampilkan kontrolnya. Kemudian, pilih nama kontrol untuk membuka halaman detail kontrol.
4. (Opsional) Pilih Perbarui status kontrol untuk mengubah status kontrol. Saat peninjauan sedang berlangsung, Anda dapat menandai status sebagai Sedang ditinjau.
5. Tinjau informasi tentang kontrol di folder Bukti, Detail, Sumber Bukti, Komentar, dan tab Changelog. Untuk mempelajari tentang masing-masing tab ini dan cara memahami data yang dikandungnya, lihat [Meninjau kontrol penilaian di AWS Audit Manager](#).

Untuk meninjau bukti untuk kontrol

1. Dari halaman detail kontrol, pilih tab Folder Bukti.
2. Arahkan ke tabel folder Bukti, tempat daftar folder yang berisi bukti untuk kontrol tersebut ditampilkan. Folder ini diatur dan diberi nama berdasarkan tanggal ketika bukti dalam folder itu dikumpulkan.

3. Pilih nama folder bukti untuk membukanya. Dari sini, Anda dapat meninjau ringkasan semua bukti yang dikumpulkan pada tanggal itu. Untuk memahami informasi ini, lihat [Meninjau folder bukti di AWS Audit Manager](#).
4. Dari halaman ringkasan folder bukti, arahkan ke tabel Bukti. Di bawah kolom Waktu, pilih item baris untuk membuka dan meninjau detail bukti yang dikumpulkan pada waktu itu. Untuk memahami informasi ini, lihat [Meninjau bukti di AWS Audit Manager](#).

Langkah 3. Tambahkan bukti manual (opsional)

Meskipun AWS Audit Manager secara otomatis mengumpulkan bukti untuk banyak kontrol, dalam beberapa kasus Anda mungkin perlu memberikan bukti tambahan. Dalam kasus ini, Anda dapat menambahkan bukti Anda sendiri secara manual yang membantu Anda menunjukkan kepatuhan terhadap kontrol itu.

Untuk menambahkan bukti manual ke kontrol

Ada beberapa cara untuk menambahkan bukti manual ke kontrol. Anda dapat mengimpor file dari Amazon S3, mengunggah file dari browser Anda, atau memasukkan respons teks. Untuk petunjuk untuk setiap metode, lihat [Menambahkan bukti manual di AWS Audit Manager](#).

Langkah 4. Menambahkan komentar untuk kontrol (opsional)

Anda dapat menambahkan komentar untuk kontrol apa pun yang Anda tinjau. Komentar ini dapat dilihat oleh pemilik audit. Misalnya, Anda dapat meninggalkan komentar untuk memberikan pembaruan status dan mengonfirmasi bahwa Anda telah memperbaiki masalah apa pun dengan kontrol tersebut.

Untuk menambahkan komentar ke kontrol

1. Dari halaman Notifikasi, tinjau daftar kumpulan kontrol yang didelegasikan kepada Anda. Temukan kumpulan kontrol yang ingin Anda beri komentar, dan pilih nama penilaian terkait.
2. Pilih tab Kontrol, gulir ke bawah ke tabel Kumpulan kontrol, lalu pilih nama kontrol untuk membukanya.
3. Pilih tab Komentar.
4. Di bawah Kirim komentar, masukkan komentar Anda di kotak teks.
5. Pilih Kirim komentar untuk menambahkan komentar Anda. Komentar Anda sekarang muncul di bawah bagian Komentar sebelumnya di halaman, bersama dengan komentar lain mengenai kontrol ini.

Langkah 5: Tandai kontrol sebagai ditinjau (opsional)

Mengubah status kontrol adalah opsional. Namun, kami menyarankan Anda mengubah status setiap kontrol menjadi Ditinjau saat Anda menyelesaikan peninjauan untuk kontrol tersebut. Terlepas dari status setiap kontrol individu, Anda masih dapat mengirimkan kontrol ke pemilik audit.

Untuk menandai kontrol sebagai ditinjau

1. Dari halaman Notifikasi, tinjau daftar kumpulan kontrol yang didelegasikan kepada Anda. Temukan kumpulan kontrol yang berisi kontrol yang ingin Anda tandai sebagai ditinjau. Kemudian, pilih nama penilaian terkait untuk membuka halaman detail penilaian.
2. Di bawah tab Kontrol pada halaman detail penilaian, gulir ke bawah ke tabel Kumpulan kontrol.
3. Di bawah kolom Kontrol dikelompokkan berdasarkan kumpulan kontrol, perluas nama kumpulan kontrol untuk menampilkan kontrolnya. Pilih nama kontrol untuk membuka halaman detail kontrol.
4. Pilih Perbarui status kontrol dan ubah status menjadi Ditinjau.
5. Di jendela pop-up yang muncul, pilih Perbarui status kontrol untuk mengonfirmasi bahwa Anda selesai meninjau kontrol.

Langkah 6. Kirim kembali set kontrol yang ditinjau ke pemilik audit

Setelah selesai meninjau semua kontrol, kirimkan kembali set kontrol ke pemilik audit untuk memberi tahu mereka bahwa Anda telah menyelesaikan peninjauan.

Untuk mengirimkan kumpulan kontrol yang telah ditinjau kembali ke pemilik

1. Di halaman Notifikasi, tinjau daftar kumpulan kontrol yang ditetapkan untuk Anda. Temukan kumpulan kontrol yang ingin Anda kirimkan ke pemilik audit, dan pilih nama penilaian terkait.
2. Gulir ke bawah ke tabel Kumpulan kontrol, pilih kumpulan kontrol yang ingin Anda kirimkan kembali ke pemilik audit, lalu pilih Kirim untuk ditinjau.
3. Di jendela pop-up yang muncul, Anda dapat menambahkan komentar tingkat tinggi tentang kumpulan kontrol tersebut sebelum memilih Kirim untuk ditinjau.

Setelah Anda mengirimkan kontrol ke pemilik audit, pemilik audit dapat melihat komentar apa pun yang Anda tinggalkan untuk pemilik audit.

Sumber daya tambahan

Anda dapat terus mempelajari lebih lanjut tentang konsep yang diperkenalkan dalam tutorial ini. Berikut adalah beberapa sumber daya yang direkomendasikan:

- [Meninjau detail penilaian di AWS Audit Manager](#)- Memperkenalkan Anda ke halaman detail penilaian, di mana Anda dapat menjelajahi berbagai komponen penilaian Manajer Audit.
- [Meninjau kontrol penilaian di AWS Audit Manager](#) dan [Meninjau bukti di AWS Audit Manager](#) - Memberikan definisi untuk membantu Anda memahami kontrol dan bukti dalam penilaian.
- [Memahami AWS Audit Manager konsep dan terminologi](#)- Memberikan definisi untuk konsep dan terminologi yang digunakan dalam Audit Manager.

Menggunakan dasbor Audit Manager

Dengan dasbor Audit Manager, Anda dapat memvisualisasikan bukti yang tidak sesuai dalam penilaian aktif Anda. Ini adalah cara yang mudah dan cepat untuk memantau penilaian Anda, tetap mendapat informasi, dan memperbaiki masalah secara proaktif. Secara default, dasbor menyediakan tampilan agregat dari atas ke bawah dari semua penilaian aktif Anda. Dengan menggunakan tampilan ini, Anda dapat mengidentifikasi masalah dalam penilaian Anda secara visual tanpa terlebih dahulu perlu menyaring sejumlah besar bukti individu.

Dasbor adalah layar pertama yang Anda lihat saat masuk ke konsol Audit Manager. Ini berisi dua widget yang menunjukkan data dan indikator kinerja utama (KPI) yang paling relevan bagi Anda. Menggunakan filter penilaian, Anda dapat menyempurnakan data ini untuk fokus pada KPI untuk penilaian tertentu. Dari sana, Anda dapat meninjau pengelompokan domain kontrol untuk mengidentifikasi kontrol mana yang memiliki bukti paling tidak sesuai. Kemudian, Anda dapat menjelajahi kontrol yang mendasarinya untuk memeriksa dan memperbaiki masalah.

Note

Jika Anda adalah pengguna Audit Manager pertama kali atau Anda tidak memiliki penilaian aktif, tidak ada data yang ditampilkan di dasbor. Untuk memulai, [buat penilaian](#). Ini memulai pengumpulan bukti yang sedang berlangsung. Setelah periode 24 jam, data bukti agregat akan mulai muncul di dasbor. Anda dapat membaca bagian berikut untuk mempelajari cara memahami dan menafsirkan data ini.

Halaman ini mencakup topik-topik berikut:

Topik

- [Konsep dan terminologi dasbor](#)
- [Elemen dasbor](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Konsep dan terminologi dasbor

Bagian ini mencakup hal-hal penting yang perlu diketahui tentang dasbor Audit Manager sebelum Anda mulai menggunakannya.

Izin dan visibilitas

Baik pemilik [audit](#) maupun [delegasi](#) memiliki akses ke dasbor. Ini berarti bahwa kedua persona ini dapat melihat metrik dan agregat untuk semua penilaian aktif di Anda. Akun AWS Memiliki akses ke informasi yang sama memungkinkan semua tim Anda untuk fokus pada KPI dan tujuan yang sama.

Filter

Audit Manager menyediakan tingkat halaman [the section called “Filter penilaian”](#) yang dapat Anda terapkan ke semua widget di dasbor Anda.

Non-compliant bukti

Dasbor menyoroti kontrol dalam penilaian Anda yang memiliki bukti pemeriksaan [kepatuhan](#) dengan kesimpulan yang tidak sesuai. Bukti pemeriksaan kepatuhan berkaitan dengan kontrol yang menggunakan AWS Config atau AWS Security Hub CSPM sebagai jenis sumber data. Untuk jenis bukti ini, Manajer Audit melaporkan hasil pemeriksaan kepatuhan langsung dari layanan tersebut. Jika Security Hub CSPM melaporkan hasil Gag al, atau jika AWS Config melaporkan Non-compliant hasilnya, Audit Manager mengklasifikasikan bukti sebagai tidak sesuai.

Bukti tidak meyakinkan

Bukti tidak meyakinkan jika pemeriksaan kepatuhan tidak tersedia atau berlaku. Akibatnya, tidak ada evaluasi kepatuhan yang dapat dilakukan. Ini terjadi jika kontrol menggunakan AWS Config atau AWS Security Hub CSPM sebagai tipe sumber data tetapi Anda tidak mengaktifkan layanan tersebut. Ini juga terjadi jika kontrol menggunakan tipe sumber data yang tidak mendukung pemeriksaan kepatuhan, seperti bukti manual, panggilan AWS API, atau AWS CloudTrail. Di konsol, bukti dengan status pemeriksaan kepatuhan tidak berlaku diklasifikasikan sebagai tidak meyakinkan di dasbor.

Anda dapat menggunakan bukti yang tidak meyakinkan untuk mengevaluasi kepatuhan kontrol secara manual.

 Note

Bukti yang tidak meyakinkan tidak menunjukkan kegagalan, itu menandakan bahwa Anda harus mengevaluasi bukti kepatuhan secara manual.

Bukti yang sesuai

Bukti sesuai jika pemeriksaan kepatuhan melaporkan tidak ada masalah. Ini adalah kasus jika Security Hub CSPM melaporkan hasil Pass, atau AWS Config melaporkan hasil Compliant.

Kontrol domain

Dasbor memperkenalkan konsep domain kontrol. Anda dapat menganggap domain kontrol sebagai kategori umum kontrol yang tidak spesifik untuk satu kerangka kerja. Pengelompokan domain kontrol adalah salah satu fitur dasbor yang paling kuat. Audit Manager menyoroti kontrol dalam penilaian Anda yang memiliki bukti yang tidak sesuai, dan mengelompokkannya berdasarkan domain kontrol. Dengan menggunakan fitur ini, Anda dapat memfokuskan upaya remediasi Anda pada domain subjek tertentu saat Anda mempersiapkan audit.

 Note

Domain kontrol berbeda dengan kumpulan kontrol. Kumpulan kontrol adalah pengelompokan kontrol khusus kerangka kerja yang biasanya ditentukan oleh badan pengatur. Misalnya, kerangka kerja PCI DSS memiliki kumpulan kontrol bernama Per syarat 8: Identifikasi dan otentikasi akses ke komponen sistem. Kumpulan kontrol ini berada di bawah domain kontrol Identitas dan manajemen akses.

Konsistensi data akhirnya

Data dasbor akhirnya konsisten. Ini berarti bahwa, ketika Anda membaca data dari dasbor, itu mungkin tidak langsung mencerminkan hasil operasi penulisan atau pembaruan yang baru saja selesai. Jika Anda memeriksa lagi dalam beberapa jam, dasbor harus mencerminkan data terbaru.

Data dari penilaian yang dihapus dan tidak aktif

Dasbor menampilkan data dari penilaian aktif. Jika Anda menghapus penilaian atau mengubah statusnya menjadi tidak aktif pada hari yang sama saat Anda melihat dasbor, data akan disertakan untuk penilaian tersebut sebagai berikut.

- **Penilaian tidak aktif** — Jika Manajer Audit mengumpulkan bukti untuk penilaian Anda sebelum Anda mengubahnya menjadi tidak aktif, data bukti tersebut disertakan dalam hitungan dasbor untuk hari itu.
- **Penilaian yang dihapus** — Jika Manajer Audit mengumpulkan bukti untuk penilaian Anda sebelum Anda menghapusnya, data bukti tersebut tidak disertakan dalam hitungan dasbor untuk hari itu.

Elemen dasbor

Bagian berikut mencakup berbagai komponen dasbor.

Topik

- [Filter penilaian](#)
- [Cuplikan harian](#)
- [Kontrol dengan bukti yang tidak sesuai dikelompokkan berdasarkan domain kontrol](#)

Filter penilaian

Anda dapat menggunakan filter penilaian untuk fokus pada penilaian aktif tertentu.

Secara default, dasbor menampilkan data agregat untuk semua penilaian aktif Anda. Jika Anda ingin melihat data untuk penilaian tertentu, Anda menerapkan filter penilaian. Ini adalah filter tingkat halaman yang berlaku untuk semua widget di dasbor.



Untuk menerapkan filter penilaian, pilih penilaian dari daftar drop-down di bagian atas dasbor. Daftar ini menampilkan hingga 10 penilaian aktif Anda. Penilaian yang paling baru dibuat muncul pertama kali. Jika Anda memiliki banyak penilaian aktif, Anda dapat mulai mengetik nama penilaian untuk menemukannya dengan cepat. Setelah Anda memilih penilaian, dasbor menampilkan data untuk penilaian itu saja.

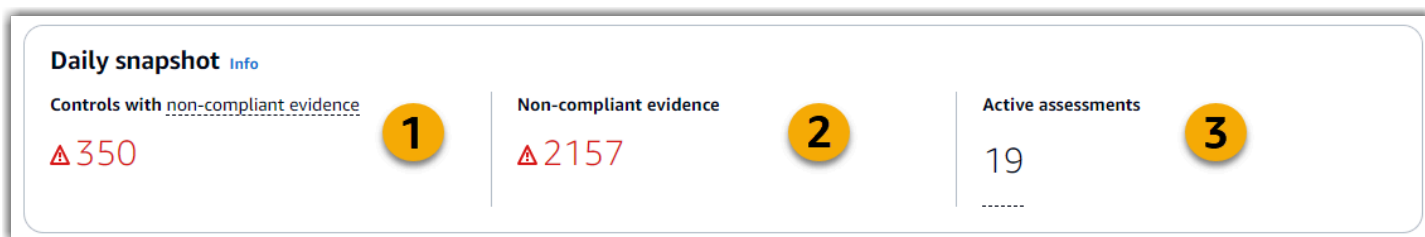
Cuplikan harian

Widget ini menampilkan snapshot status kepatuhan saat ini dari penilaian aktif Anda.

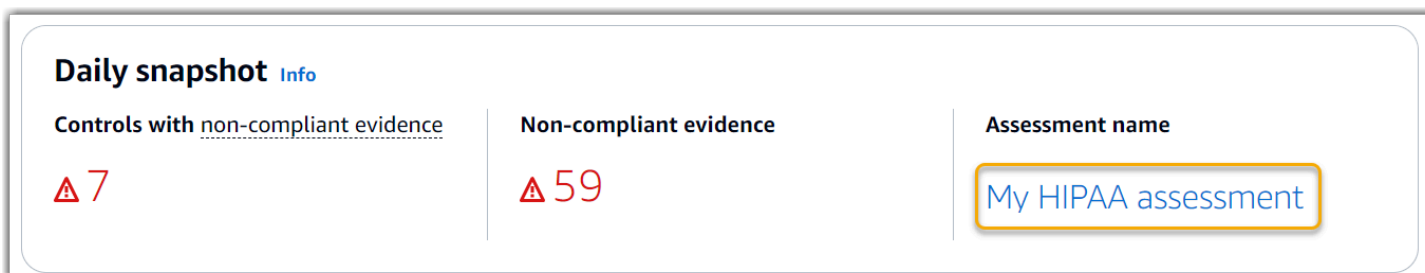
Snapshot harian mencerminkan data terbaru yang dikumpulkan pada tanggal di bagian atas dasbor. Tanggal dan waktu di dasbor diwakili dalam Coordinated Universal Time (UTC). Penting untuk dipahami bahwa angka-angka ini adalah hitungan harian berdasarkan stempel waktu ini. Mereka bukan jumlah total sampai saat ini.

Secara default, snapshot harian menampilkan data berikut untuk semua penilaian aktif Anda:

1. Kontrol dengan bukti yang tidak sesuai - Jumlah total kontrol yang terkait dengan bukti yang tidak sesuai.
2. Non-compliant bukti - Jumlah total bukti pemeriksaan kepatuhan dengan kesimpulan yang tidak sesuai.
3. Penilaian aktif - Jumlah total penilaian aktif Anda. Pilih nomor ini untuk melihat tautan ke penilaian ini.



Data snapshot harian berubah berdasarkan [the section called “Filter penilaian”](#) yang Anda terapkan. Saat Anda menentukan penilaian, data mencerminkan jumlah harian untuk penilaian itu saja. Dalam hal ini, snapshot harian menunjukkan nama penilaian yang Anda tentukan. Anda dapat memilih nama penilaian untuk membukanya.

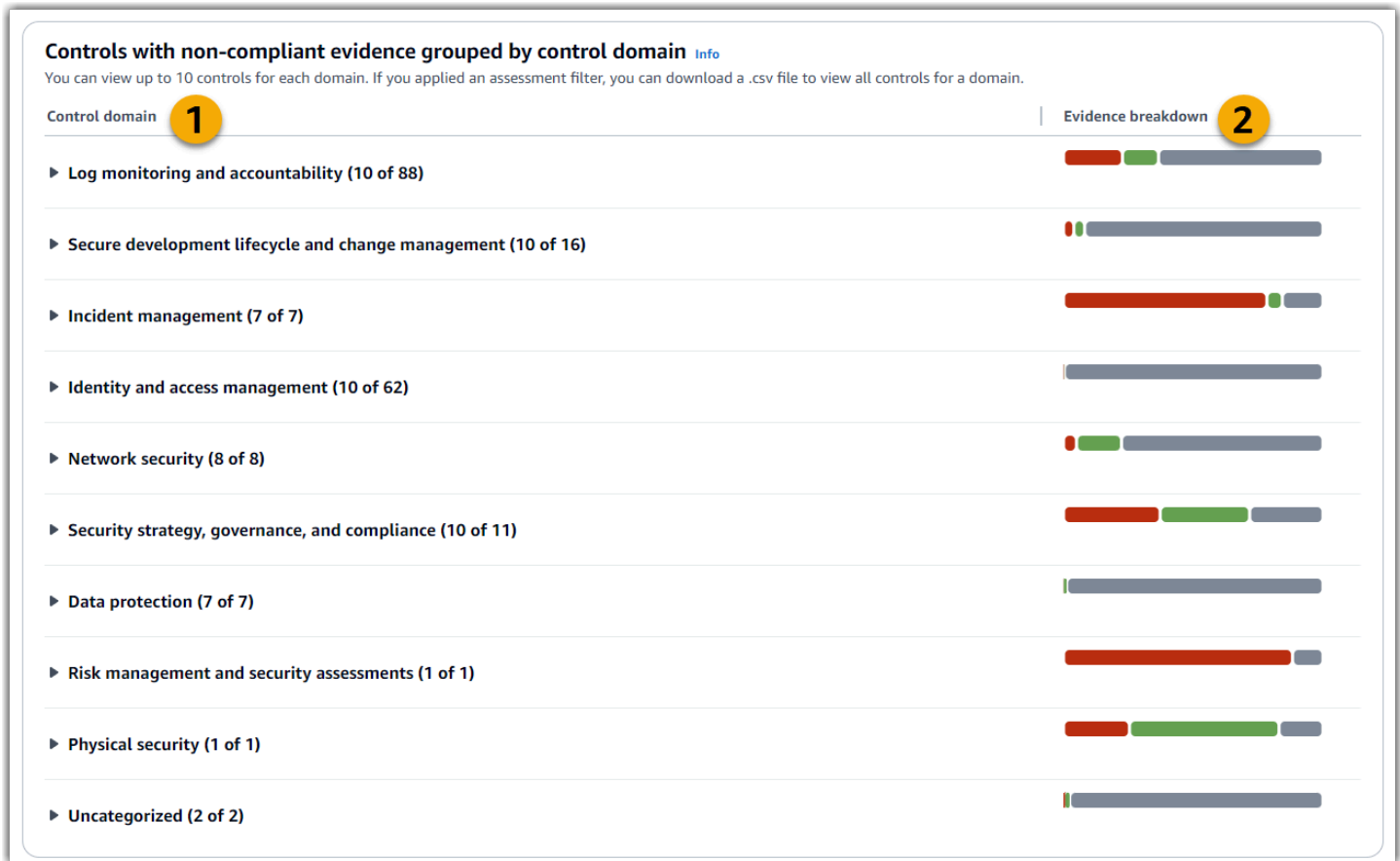


Kontrol dengan bukti yang tidak sesuai dikelompokkan berdasarkan domain kontrol

Anda dapat menggunakan widget ini untuk mengidentifikasi kontrol mana yang memiliki bukti paling tidak sesuai.

Secara default, widget menampilkan data berikut untuk semua penilaian aktif Anda:

1. Domain kontrol — Daftar [control domains](#) yang terkait dengan penilaian aktif Anda.
2. Rincian bukti — Bagan batang yang menunjukkan rincian status kepatuhan bukti.



Untuk memperluas domain kontrol, pilih panah di sebelah namanya. Saat diperluas, konsol menampilkan hingga 10 kontrol untuk setiap domain. Kontrol ini diberi peringkat sesuai dengan jumlah total tertinggi bukti yang tidak sesuai.

Data dalam widget ini berubah berdasarkan [the section called “Filter penilaian”](#) yang Anda terapkan. Saat Anda menentukan penilaian, Anda melihat data untuk penilaian itu saja. Selain itu, Anda juga dapat mengunduh file CSV untuk setiap domain kontrol yang tersedia dalam penilaian.

Controls with non-compliant evidence grouped by control domain [Info](#)

You can view up to 10 controls for each domain. If you applied an assessment filter, you can download a .csv file to view all controls for a domain.

Control domain	Evidence breakdown	CSV
▼ Log monitoring and accountability (2 of 2)		Download
Smpl-1.0.1: CloudTrail Instance Events		
Smpl-1.0.2: CloudTrail Volume Events		
► Identity and access management (1 of 1)		Download

File CSV menyertakan daftar lengkap kontrol di domain yang terkait dengan bukti yang tidak sesuai. Contoh berikut menunjukkan kolom data CSV dengan nilai fiksi.

	A	B	C	D	E	F	G
1	Date and Time	AssessmentID	AssessmentName	ControlId	ControlName	ControlDescription	DataSource
2	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	abcdefg-1234-bcde-5678-cdefghijklmn	Control 1	Description of control 1	Manual
3	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	12345678-abcd-9012-bcde-345678901234	Control 2	Description of control 2	Manual
4	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	bcdefghi-2345-cdef-3456-defghijklmno	Control 3	Description of control 3	AWS Config, AWS Security Hub
5	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	23456789-bcde-0123-cdef-456789012345	Control 4	Description of control 4	Manual
6	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	cdefghij-3456-defg-4567-efghijklmnop	Control 5	Description of control 5	AWS Config
7	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	34567890-cdef-1234-defg-567890123456	Control 6	Description of control 6	Manual
8	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	defghijk-4567-efgh-5678-fghijklmnopq	Control 7	Description of control 7	AWS Config
9	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	45678901-defg-2345-efgh-678901234567	Control 8	Description of control 8	AWS Security Hub
10	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	efghijkl-5678-fghi-6789-ghijklmnopqr	Control 9	Description of control 9	Manual
11	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	56789012-efgh-3456-fghi-789012345678	Control 10	Description of control 10	Manual
12	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	fghijklm-6789-ghij-7890-hijklmnopqrs	Control 11	Description of control 11	Manual
13	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	67890123-fghi-4567-ghij-890123456789	Control 12	Description of control 12	Manual
14	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	ghijklmn-7890-hijk-8901-ijklmnopqrst	Control 13	Description of control 13	AWS Config, AWS Security Hub
15	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	78901234-ghij-5678-hijk-901234567890	Control 14	Description of control 14	Manual
16							

Terakhir, ketika Anda menerapkan filter penilaian, nama kontrol di bawah setiap domain akan ditautkan. Pilih kontrol apa pun untuk membuka halaman detail kontrol dalam penilaian yang ditentukan.

Controls with non-compliant evidence grouped by control domain [Info](#)

You can view up to 10 controls for each domain. If you applied an assessment filter, you can download a .csv file to view all controls for a domain.

Control domain	Evidence breakdown	CSV
▼ Log monitoring and accountability (2 of 2)		Download
Smpl-1.0.1: CloudTrail Instance Events		
Smpl-1.0.2: CloudTrail Volume Events		
► Identity and access management (1 of 1)		Download

 Tip

Menggunakan halaman detail kontrol sebagai titik awal Anda, Anda dapat berpindah dari satu tingkat detail ke tingkat berikutnya.

1. Halaman detail kontrol - Di halaman ini, [Tab Folder Bukti](#) daftar folder bukti harian yang dikumpulkan oleh Manajer Audit untuk kontrol itu. Untuk detail lebih lanjut, pilih folder.
2. Folder bukti - Selanjutnya, Anda dapat [Ringkasan folder bukti](#) meninjau dan daftar bukti di folder itu. Untuk detail lebih lanjut, pilih item bukti individu.
3. Bukti individu - Terakhir, Anda dapat menjelajahi detail bukti [individu](#). Ini adalah tingkat data bukti yang paling terperinci.

Langkah selanjutnya

Berikut adalah beberapa langkah selanjutnya yang dapat Anda ambil setelah meninjau dasbor.

- Unduh file CSV — Temukan domain penilaian dan kontrol yang ingin Anda fokuskan, dan [unduh daftar lengkap kontrol terkait dengan bukti](#) yang tidak sesuai.
- Meninjau kontrol — Setelah mengidentifikasi kontrol yang memerlukan perbaikan, Anda dapat men [injau kontrol](#) tersebut.
- Mendelegasikan kontrol untuk ditinjau — Jika Anda memerlukan bantuan untuk meninjau kontrol, Anda dapat [mendelegasikan kumpulan kontrol untuk ditinjau](#).
- Mengedit penilaian Anda — Jika Anda ingin mengubah ruang lingkup penilaian aktif, Anda dapat [mengedit penilaian](#).
- Perbarui status penilaian Anda — Jika Anda ingin berhenti mengumpulkan bukti untuk penilaian, Anda dapat [mengubah status penilaian menjadi tidak aktif](#).

Sumber daya tambahan

Untuk menemukan jawaban atas pertanyaan dan masalah umum, lihat [Memecahkan masalah dasbor](#) di bagian Pemecahan Masalah pada panduan ini.

Mengelola penilaian di AWS Audit Manager

Penilaian Manajer Audit didasarkan pada kerangka kerja, yang merupakan pengelompokan kontrol. Menggunakan kerangka kerja sebagai titik awal, Anda dapat membuat penilaian yang mengumpulkan bukti untuk kontrol dalam kerangka itu. Dalam penilaian Anda, Anda juga dapat menentukan ruang lingkup audit Anda. Ini termasuk menentukan bukti Akun AWS yang ingin Anda kumpulkan.

Poin kunci

Anda dapat membuat penilaian dari kerangka kerja apa pun. Entah, Anda dapat menggunakan kerangka [kerja standar](#) yang disediakan oleh Audit Manager. Atau, Anda dapat membuat penilaian dari kerangka [kerja khusus](#) yang Anda buat sendiri. Kerangka kerja standar berisi kumpulan kontrol bawaan yang mendukung standar kepatuhan atau peraturan tertentu. Sebaliknya, kerangka kerja khusus berisi kontrol yang dapat Anda sesuaikan dan kelompokkan sesuai dengan kebutuhan Anda sendiri.

Ketika Anda membuat penilaian, ini memulai pengumpulan bukti yang sedang berlangsung. Ketika tiba waktunya untuk audit, Anda atau delegasi dapat men [injau bukti ini](#) dan kemudian men [ambahkannya ke laporan penilaian](#).

Note

AWS Audit Manager membantu mengumpulkan bukti yang relevan untuk memverifikasi kepatuhan terhadap standar dan peraturan kepatuhan tertentu. Namun, itu tidak menilai kepatuhan Anda sendiri. Bukti yang dikumpulkan oleh AWS Audit Manager karena itu mungkin tidak mencakup semua informasi tentang AWS penggunaan Anda yang diperlukan untuk audit. AWS Audit Manager bukan pengganti penasihat hukum atau pakar kepatuhan.

Sumber daya tambahan

Untuk membuat dan mengelola penilaian di Audit Manager, ikuti prosedur yang diuraikan di sini.

- [Membuat penilaian di AWS Audit Manager](#)

- [Menemukan penilaian Anda di AWS Audit Manager](#)
- [Meninjau penilaian di AWS Audit Manager](#)
 - [Meninjau detail penilaian di AWS Audit Manager](#)
 - [Meninjau kontrol penilaian di AWS Audit Manager](#)
 - [Meninjau folder bukti di AWS Audit Manager](#)
 - [Meninjau bukti di AWS Audit Manager](#)
- [Mengedit penilaian di AWS Audit Manager](#)
 - [Mengubah status kontrol penilaian di AWS Audit Manager](#)
 - [Mengubah status penilaian menjadi tidak aktif di AWS Audit Manager](#)
- [Menambahkan bukti manual di AWS Audit Manager](#)
 - [Mengimpor file bukti manual dari Amazon S3](#)
 - [Mengunggah file bukti manual dari browser Anda](#)
 - [Memasukkan tanggapan teks bentuk bebas sebagai bukti manual](#)
 - [Format file yang didukung untuk bukti manual](#)
- [Menyiapkan laporan penilaian di AWS Audit Manager](#)
 - [Menambahkan bukti ke laporan penilaian](#)
 - [Menghapus bukti dari laporan penilaian](#)
 - [Menghasilkan laporan penilaian](#)
 - [Mengunduh laporan penilaian dari pusat unduhan](#)
 - [Menavigasi laporan penilaian dan menjelajahi isinya](#)
 - [Memvalidasi laporan penilaian](#)
 - [Menghapus laporan penilaian](#)
 - [Menghasilkan laporan penilaian dari hasil pencarian pencari bukti](#)
- [Menghapus penilaian di AWS Audit Manager](#)

Membuat penilaian di AWS Audit Manager

Topik ini dibangun di atas [Tutorial untuk Pemilik Audit: Membuat penilaian](#). Anda akan menemukan petunjuk terperinci di halaman ini yang menunjukkan cara membuat penilaian dari kerangka kerja. Ikuti langkah-langkah ini untuk membuat penilaian dan memulai pengumpulan bukti yang sedang berlangsung.

Prasyarat

Sebelum memulai tutorial ini, pastikan Anda memenuhi persyaratan berikut:

- Anda menyelesaikan semua prasyarat yang dijelaskan di [Pengaturan AWS Audit Manager dengan pengaturan yang disarankan](#). Anda harus menggunakan konsol Anda Akun AWS dan Audit Manager untuk menyelesaikan tutorial ini.
- Identitas IAM Anda memiliki izin yang sesuai untuk membuat dan mengelola penilaian di Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Tugas

- [Langkah 1: Tentukan detail penilaian](#)
- [Langkah 2: Tentukan Akun AWS dalam ruang lingkup](#)
- [Langkah 3: Tentukan pemilik audit](#)
 - [Izin pemilik audit](#)
- [Langkah 4: Tinjau dan buat](#)

Langkah 1: Tentukan detail penilaian

Mulailah dengan memilih kerangka kerja dan memberikan informasi dasar untuk penilaian Anda.

Untuk menentukan detail penilaian

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi, pilih **Penilaian**, lalu pilih **Buat penilaian**.
3. Di bawah **Nama**, masukkan nama untuk penilaian Anda.
4. (Opsional) Di bawah **Deskripsi**, masukkan deskripsi untuk penilaian Anda.
5. Di bawah **Tujuan laporan penilaian**, pilih bucket S3 tempat Anda ingin menyimpan laporan penilaian Anda.

 Tip

Tujuan laporan penilaian default didasarkan pada pengaturan [penilaian Anda](#). Jika mau, Anda dapat membuat dan menggunakan beberapa bucket S3 untuk membantu mengatur laporan penilaian untuk penilaian yang berbeda. AWS Audit Manager mendukung ekspor laporan penilaian ke bucket Amazon S3, termasuk tujuan lintas akun. Untuk keamanan dan kinerja yang optimal, sebaiknya gunakan bucket S3 di AWS akun dan wilayah yang sama dengan penilaian Anda.

6. Di bawah **Pilih kerangka kerja**, pilih kerangka kerja yang ingin Anda buat penilaian. Anda juga dapat menggunakan bilah pencarian untuk mencari kerangka kerja berdasarkan nama, atau dengan standar kepatuhan atau peraturan.

 Tip

Untuk mempelajari lebih lanjut tentang kerangka kerja, pilih nama kerangka kerja untuk melihat halaman detail kerangka kerja.

7. (Opsional) Di bawah **Tag**, pilih **Tambahkan tag baru** untuk mengaitkan tag dengan penilaian Anda. Anda dapat menentukan kunci dan nilai untuk setiap tag. Kunci tag adalah wajib dan dapat digunakan sebagai kriteria pencarian saat Anda mencari penilaian ini.
8. Pilih Berikutnya.

 Note

Penting untuk memastikan bahwa penilaian Anda mengumpulkan bukti yang benar untuk kerangka kerja tertentu. Sebelum Anda memulai pengumpulan bukti, kami sarankan Anda meninjau persyaratan untuk kerangka kerja yang Anda pilih. Kemudian, validasi persyaratan ini terhadap parameter AWS Config aturan Anda saat ini. Untuk memastikan bahwa parameter aturan Anda selaras dengan persyaratan kerangka kerja, Anda dapat [memperbarui aturan di AWS Config](#).

Misalnya, Anda membuat penilaian untuk CIS v1.2.0. Kerangka kerja ini memiliki kontrol bernama [1.9 - Pastikan kebijakan kata sandi IAM memerlukan panjang minimum 14 atau lebih](#). Di AWS Config, [aturan](#) iam-password-policy memiliki MinimumPasswordLength parameter yang memeriksa panjang kata sandi. Nilai default untuk parameter ini adalah 14 karakter. Akibatnya, aturan selaras dengan persyaratan kontrol. Jika Anda tidak

menggunakan nilai parameter default, pastikan nilai yang Anda gunakan sama dengan atau lebih besar dari persyaratan 14 karakter dari CIS v1.2.0. Anda dapat menemukan detail parameter default untuk setiap aturan terkelola dalam [AWS Config dokumentasi](#).

Langkah 2: Tentukan Akun AWS dalam ruang lingkup

Anda dapat menentukan beberapa Akun AWS untuk berada dalam lingkup penilaian. Audit Manager mendukung beberapa akun melalui integrasi dengan AWS Organizations. Ini berarti bahwa penilaian Manajer Audit dapat dijalankan di beberapa akun, dan bukti yang dikumpulkan dikonsolidasikan ke dalam akun administrator yang didelegasikan. Untuk mengaktifkan Organisasi di Audit Manager, lihat [Aktifkan dan mengatur AWS Organizations](#).

Note

Audit Manager dapat mendukung hingga 200 akun dalam lingkup penilaian. Jika Anda mencoba memasukkan lebih dari 200 akun, pembuatan penilaian akan gagal. Selain itu, jika Anda mencoba menambahkan lebih dari 250 akun unik di semua penilaian Anda, pembuatan penilaian akan gagal.

Untuk menentukan Akun AWS dalam ruang lingkup

1. Di bawah Akun AWS, pilih Akun AWS yang ingin Anda sertakan dalam lingkup penilaian Anda.
 - Jika Anda mengaktifkan Organisasi di Audit Manager, beberapa akun akan ditampilkan. Anda dapat memilih satu atau lebih akun dari daftar. Atau, Anda juga dapat mencari akun berdasarkan nama akun, ID, atau email.
 - Jika Anda tidak mengaktifkan Organisasi di Manajer Audit, hanya saat Akun AWS ini yang terdaftar.
2. Pilih Berikutnya.

Note

Ketika akun dalam lingkup dihapus dari organisasi Anda, Manajer Audit tidak lagi mengumpulkan bukti untuk akun tersebut. Namun, akun terus ditampilkan dalam penilaian Anda di bawah Akun AWS tab. Untuk menghapus akun dari daftar akun dalam cakupan, [edit](#)

[penilaian](#). Akun yang dihapus tidak lagi ditampilkan dalam daftar selama pengeditan, dan Anda dapat menyimpan perubahan tanpa akun tersebut dalam cakupan.

Langkah 3: Tentukan pemilik audit

Pada langkah ini, Anda menentukan pemilik audit untuk penilaian Anda. Pemilik audit adalah individu di tempat kerja Anda—biasanya dari GRC, SecOps, atau DevOps tim—yang bertanggung jawab untuk mengelola penilaian Manajer Audit. Kami menyarankan agar mereka menggunakan [AWSAuditManagerAdministratorAccess](#) kebijakan tersebut.

Untuk menentukan pemilik audit

1. Di bawah Pemilik audit, tinjau daftar pemilik audit saat ini. Kolom Audit owner menampilkan ID pengguna dan peran. Akun AWS Kolom menampilkan Akun AWS pemilik audit tersebut.
2. Pemilik audit yang memiliki kotak centang yang dipilih disertakan dalam penilaian Anda. Kosongkan kotak centang untuk setiap pemilik audit untuk menghapusnya dari penilaian. Anda dapat menemukan pemilik audit tambahan dengan menggunakan bilah pencarian untuk mencari berdasarkan nama atau Akun AWS.
3. Setelah selesai, pilih Berikutnya.

Izin pemilik audit

Kebijakan di bawah ini dilampirkan untuk semua pemilik audit penilaian.

Audit Manager menggantinya *placeholder text* dengan pengidentifikasi akun dan sumber daya Anda sebelum melampirkan kebijakan.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AuditOwner",
      "Effect": "Allow",
      "Principal": {
        "AWS": "Principal for user/role who are the audit owners of the Assessment"
      }
    }
  ]
}
```

```

    },
    "Action": [
        "auditmanager:GetAssessment",
        "auditmanager:UpdateAssessment",
        "auditmanager:UpdateAssessmentControlSetStatus",
        "auditmanager:UpdateAssessmentStatus",
        "auditmanager:UpdateAssessmentControl",
        "auditmanager>DeleteAssessment",
        "auditmanager:GetChangeLogs",
        "auditmanager:GetEvidenceFoldersByAssessment",
        "auditmanager:GetEvidenceFoldersByAssessmentControl",
        "auditmanager:BatchImportEvidenceToAssessmentControl",
        "auditmanager:GetEvidenceFolder",
        "auditmanager:GetEvidence",
        "auditmanager:GetEvidenceByEvidenceFolder",
        "auditmanager:BatchCreateDelegationByAssessment",
        "auditmanager:BatchDeleteDelegationByAssessment",
        "auditmanager:AssociateAssessmentReportEvidenceFolder",
        "auditmanager:BatchAssociateAssessmentReportEvidence",
        "auditmanager:BatchDisassociateAssessmentReportEvidence",
        "auditmanager>CreateAssessmentReport",
        "auditmanager>DeleteAssessmentReport",
        "auditmanager:DisassociateAssessmentReportEvidenceFolder",
        "auditmanager:GetAssessmentReportUrl"
    ],
    "Resource": [
        "arn:aws:auditmanager:us-east-1:123456789012:assessment/assessment_ID",
        "arn:aws:auditmanager:us-east-1:123456789012:assessment/assessment_ID/*"
    ]
}

```

Langkah 4: Tinjau dan buat

Tinjau informasi untuk penilaian Anda. Untuk mengubah informasi untuk satu langkah, pilih **Edit**. Setelah selesai, pilih **Buat penilaian**.

Tindakan ini memulai pengumpulan bukti yang sedang berlangsung untuk penilaian Anda. Setelah Anda membuat penilaian, pengumpulan bukti berlanjut hingga Anda [mengubah status penilaian](#)

menjadi tidak aktif. Atau, Anda dapat menghentikan pengumpulan bukti untuk kontrol tertentu dengan [mengubah status kontrol](#) menjadi tidak aktif.

 Note

Bukti otomatis tersedia 24 jam setelah penilaian Anda dibuat. Audit Manager secara otomatis mengumpulkan bukti dari berbagai sumber data, dan frekuensi pengumpulan bukti tersebut didasarkan pada jenis bukti. Untuk mempelajari lebih lanjut, lihat [Frekuensi pengumpulan bukti](#) di panduan ini.

Langkah selanjutnya

Untuk meninjau kembali penilaian Anda di kemudian hari, lihat [Menemukan penilaian Anda di AWS Audit Manager](#). Anda dapat mengikuti langkah-langkah ini untuk menemukan penilaian Anda sehingga Anda dapat melihat, mengedit, atau terus mengerjakannya.

Sumber daya tambahan

Untuk solusi untuk masalah penilaian di Manajer Audit, lihat [Memecahkan masalah penilaian dan pengumpulan bukti](#).

Menemukan penilaian Anda di AWS Audit Manager

Setelah membuat penilaian di AWS Audit Manager, Anda dapat menemukannya di halaman penilaian konsol Audit Manager.

Dari halaman ini, Anda dapat melakukan berbagai tindakan pada penilaian Anda. Misalnya, Anda dapat melihat detail penilaian, mengedit konfigurasi penilaian, atau menghapus penilaian yang tidak lagi diperlukan. Selain itu, halaman penilaian berfungsi sebagai titik awal untuk membuat penilaian baru.

Anda juga dapat melihat penilaian Anda secara terprogram menggunakan Audit Manager API atau AWS Command Line Interface (AWS CLI).

Prasyarat

Prosedur berikut mengasumsikan bahwa Anda sebelumnya telah membuat setidaknya satu penilaian. Jika Anda belum membuat penilaian, Anda tidak akan melihat hasil apa pun saat mengikuti langkah-langkah ini.

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk melihat penilaian di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Anda dapat melihat penilaian Anda menggunakan konsol Audit Manager, API Manajer Audit, atau AWS Command Line Interface (AWS CLI).

Audit Manager console

Untuk melihat penilaian Anda di konsol Audit Manager

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi kiri, pilih Penilaian untuk melihat daftar penilaian Anda.
3. Pilih nama penilaian apa pun untuk melihat detail penilaian tersebut.

AWS CLI

Untuk melihat penilaian Anda (CLI)

Untuk melihat penilaian di Audit Manager, jalankan perintah [list-assessment](#). Anda dapat menggunakan `--status` subperintah untuk melihat penilaian yang aktif atau tidak aktif.

```
aws auditmanager list-assessments --status ACTIVE
```

```
aws auditmanager list-assessments --status INACTIVE
```

Audit Manager API

Untuk melihat penilaian Anda menggunakan API

Untuk melihat penilaian di Audit Manager, gunakan [ListAssessments](#) operasi. Anda dapat menggunakan [atribut](#) status untuk melihat penilaian yang aktif atau tidak aktif.

Untuk informasi selengkapnya, pilih salah satu tautan sebelumnya untuk membaca lebih lanjut di Refer AWS Audit Manager ensi API. Ini termasuk informasi tentang cara menggunakan `ListAssessments` operasi dan parameter di salah satu SDK khusus bahasa AWS .

Langkah selanjutnya

Saat Anda siap untuk menjelajahi isi penilaian Anda, ikuti langkah-langkah di [Meninjau penilaian di AWS Audit Manager](#). Halaman ini akan memandu Anda melalui detail penilaian dan menjelaskan informasi yang Anda lihat di sana.

Dari halaman penilaian, Anda juga dapat [mengedit penilaian](#), [menghapus penilaian](#), atau [membuat penilaian](#).

Sumber daya tambahan

Untuk solusi masalah penilaian di Audit Manager, lihat [Memecahkan masalah penilaian dan pengumpulan bukti](#).

Meninjau penilaian di AWS Audit Manager

Setelah membuat penilaian di Audit Manager, Anda dapat membuka dan meninjau penilaian kapan saja.

Poin kunci

Ketika Anda siap untuk mengeksplorasi penilaian Anda, Anda dapat secara bertahap menyelami lebih dalam detail dan meninjau penilaian Anda dengan tingkat perincian yang meningkat.

1. Rincian penilaian — Mulailah dengan meninjau detail keseluruhan penilaian Anda. Di halaman ini Anda dapat meninjau nama penilaian, deskripsi, ruang lingkup, dan detail lainnya. Ini memberi Anda gambaran penilaian tingkat tinggi.
2. Rincian kontrol penilaian — Selanjutnya, selami lebih dalam penilaian dengan meninjau detail setiap kontrol penilaian. Ini akan memungkinkan Anda untuk memahami persyaratan dan tujuan spesifik dari setiap kontrol.

3. **Detail folder bukti** — Untuk setiap kontrol penilaian, Anda dapat meninjau folder bukti yang sesuai yang berisi bukti untuk kontrol tertentu. Folder ini mengatur bukti pendukung yang terkait dengan setiap kontrol.
4. **Detail bukti** — Terakhir, telusuri lebih lanjut untuk meninjau setiap bukti dalam setiap folder. Ini mungkin termasuk snapshot konfigurasi, log aktivitas pengguna, temuan kepatuhan, atau bukti yang diunggah secara manual seperti dokumen dan tangkapan layar. Meninjau bukti ini akan membantu Anda memahami bagaimana organisasi Anda memenuhi persyaratan kontrol.

Dengan mengikuti langkah-langkah ini, Anda dapat menjelajahi penilaian Anda secara menyeluruh, memahami komponennya, dan meninjau bukti yang mendukung upaya kepatuhan organisasi Anda.

Sumber daya tambahan

Untuk memulai meninjau penilaian di Audit Manager, ikuti prosedur yang diuraikan di sini.

- [Meninjau detail penilaian di AWS Audit Manager](#)
- [Meninjau kontrol penilaian di AWS Audit Manager](#)
- [Meninjau folder bukti di AWS Audit Manager](#)
- [Meninjau bukti di AWS Audit Manager](#)

Meninjau detail penilaian di AWS Audit Manager

Ketika Anda perlu meninjau detail penilaian, Anda akan menemukan informasi yang disusun menjadi beberapa bagian di halaman detail penilaian. Bagian ini membantu Anda dengan mudah mengakses dan memahami informasi yang relevan untuk tugas Anda.

Daftar Isi

- [Prasyarat](#)
- [Prosedur](#)
 - [Bagian rincian penilaian](#)
 - [Tab kontrol](#)
 - [Tab pemilihan laporan penilaian](#)
 - [Akun AWS tab](#)
 - [Layanan AWS tab](#)

- [Tab pemilik audit](#)
- [Tab tag](#)
- [Tab Changelog](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Prasyarat

Prosedur berikut mengasumsikan bahwa Anda sebelumnya telah membuat setidaknya satu penilaian. Jika Anda belum membuat penilaian, Anda tidak akan melihat hasil apa pun saat mengikuti langkah-langkah ini.

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk melihat penilaian di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Untuk membuka dan meninjau halaman detail penilaian

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi kiri, pilih Penilaian untuk melihat daftar penilaian Anda.
3. Pilih nama penilaian untuk membukanya.
4. Tinjau detail penilaian menggunakan informasi berikut sebagai referensi.

Bagian dari halaman detail penilaian

- [Bagian rincian penilaian](#)
- [Tab kontrol](#)
- [Tab pemilihan laporan penilaian](#)
- [Akun AWS tab](#)
- [Layanan AWS tab](#)
- [Tab pemilik audit](#)
- [Tab tag](#)

- [Tab Changelog](#)

Bagian rincian penilaian

Anda dapat menggunakan bagian Detail Penilaian untuk melihat ringkasan penilaian Anda.

The screenshot shows the 'Assessment details' section with the following fields and callouts:

- 1**: Description
- 2**: Compliance type (PCI DSS)
- 3**: Assessment reports destination (s3://bucket-name01)
- 4**: Total evidence (6715972)
- 5**: Assessment report selection (0)
- 6**: Date created (August 19, 2023, 00:51 (UTC+0:00))
- 7**: Last updated (October 17, 2023, 00:17 (UTC+0:00))
- 8**: Status (Active)

Di bagian detail penilaian, Anda dapat meninjau informasi berikut:

Nama	Deskripsi
1. Deskripsi	Deskripsi penilaian.
2. Jenis kepatuhan	Standar kepatuhan atau peraturan yang didukung penilaian.
3. Tujuan laporan penilaian	Bucket S3 tempat Audit Manager menyimpan laporan penilaian.
4. Bukti total	Jumlah total item bukti yang dikumpulkan untuk penilaian ini.
5. Pemilihan laporan penilaian	Jumlah item bukti yang dipilih untuk dimasukkan dalam laporan penilaian.
6. Tanggal dibuat	Tanggal ketika penilaian dibuat.
7. Terakhir diperbarui	Tanggal penilaian terakhir diedit.
8. Status	Status penilaian. • Aktif - Penilaian saat ini mengumpulkan bukti. • Tidak aktif - Penilaian tidak lagi mengumpulkan bukti.

Tab kontrol

Anda dapat menggunakan tab ini untuk melihat informasi tentang kontrol dalam penilaian.

Di bawah Ringkasan status Kontrol, Anda dapat meninjau informasi berikut:

Nama	Deskripsi
Kontrol total	Jumlah total kontrol dalam penilaian ini.
Diulas	Jumlah kontrol yang ditinjau oleh pemilik audit atau delegasi.
Dalam peninjauan	Jumlah kontrol yang saat ini sedang ditinjau.
Tidak aktif	Jumlah kontrol yang tidak lagi secara aktif mengumpulkan bukti

Di tabel **Kumpulan kontrol**, Anda dapat meninjau daftar kontrol yang dikelompokkan berdasarkan kumpulan kontrol. Anda dapat memperluas atau menciutkan kontrol di setiap kumpulan kontrol. Anda juga dapat mencari berdasarkan nama jika Anda mencari kontrol tertentu.

Dalam tabel ini, Anda dapat meninjau informasi berikut:

Nama	Deskripsi
Kontrol dikelompokkan berdasarkan kumpulan kontrol	Nama set kontrol.
Status kontrol	Status kontrol. - Dalam peninjauan menunjukkan bahwa kontrol ini belum ditinjau. Bukti masih dikumpulkan untuk kontrol ini, dan Anda dapat menambahkan bukti manual. Ini adalah status default. - Ditinjau menunjukkan bahwa bukti untuk kontrol ini telah ditinjau. Bukti masih dikumpulkan, dan Anda dapat menambahkan bukti manual. - Tidak aktif menunjukkan bahwa pengumpulan bukti otomatis dihentikan untuk kontrol ini. Anda tidak dapat lagi menambahkan bukti manual.
Delegasikan ke	Peninjau kontrol ini, jika ditugaskan ke delegasi untuk ditinjau.
Bukti total	Jumlah item bukti yang telah dikumpulkan untuk kontrol ini.

Tab pemilihan laporan penilaian

Anda dapat menggunakan tab ini untuk melihat bukti yang akan dimasukkan dalam laporan penilaian. Bukti dikelompokkan berdasarkan folder bukti, yang diatur berdasarkan tanggal pembuatannya.

Anda dapat menelusuri folder ini dan memilih bukti mana yang ingin Anda sertakan dalam laporan penilaian Anda. Untuk petunjuk tentang cara menambahkan bukti ke laporan penilaian, lihat [Menambahkan bukti ke laporan penilaian](#).

Di bagian ini, Anda dapat meninjau informasi berikut:

Nama	Deskripsi
Folder bukti	Nama folder bukti. Nama folder didasarkan pada tanggal ketika bukti dikumpulkan.
Bukti yang dipilih	Jumlah item bukti dalam folder yang disertakan dalam laporan penilaian.
Nama kontrol	Nama kontrol yang terkait dengan folder bukti ini.

Akun AWS tab

Anda dapat menggunakan tab ini untuk melihat Akun AWS yang ada dalam lingkup penilaian.

Di bagian ini, Anda dapat meninjau informasi berikut:

Nama	Deskripsi
ID Akun	ID dari Akun AWS.
Nama akun	Nama Akun AWS.
E-Mail	Alamat email yang terkait dengan Akun AWS.

Layanan AWS tab

Anda mungkin atau mungkin tidak melihat tab ini dalam penilaian Anda.

Jika Layanan AWS tab tidak ditampilkan (keadaan ideal)

Jika Anda tidak melihat tab ini, Manajer Audit akan mengelola yang Layanan AWS berada dalam ruang lingkup penilaian Anda.

Audit Manager menyimpulkan ruang lingkup ini dengan memeriksa kontrol penilaian Anda dan sumber datanya, dan kemudian memetakan informasi ini ke yang sesuai Layanan AWS. Setiap kali sumber data yang mendasari berubah untuk penilaian Anda, Audit Manager secara otomatis memperbarui cakupan sesuai kebutuhan untuk mencerminkan yang benar Layanan AWS. Ini memastikan bahwa penilaian Anda mengumpulkan bukti yang akurat dan komprehensif tentang semua layanan yang relevan di AWS lingkungan Anda.

Jika Layanan AWS tab ditampilkan

Jika ini, Anda melihat tab ini, Manajer Audit tidak mengelola mana yang Layanan AWS berada dalam ruang lingkup penilaian Anda.

Dalam hal ini, Anda melihat informasi berikut tentang layanan dalam lingkup yang Anda tentukan:

Nama	Deskripsi
Layanan AWS	Nama Layanan AWS.
Kategori	Kategori layanan, seperti komputasi atau database.
Deskripsi	Deskripsi Layanan AWS.

Manajer Audit melakukan penilaian sumber daya untuk layanan dalam tabel ini. Misalnya, jika Amazon S3 terdaftar, Audit Manager dapat mengumpulkan bukti tentang bucket S3 Anda. Bukti pasti yang dikumpulkan ditentukan oleh kontrol [data source](#). Misalnya, jika tipe sumber data adalah AWS Config, dan pemetaan sumber data adalah AWS Config aturan (seperti `s3-bucket-public-write-prohibited`), Audit Manager mengumpulkan hasil evaluasi aturan tersebut sebagai bukti. Untuk informasi selengkapnya, lihat [Apa perbedaan antara layanan dalam ruang lingkup dan tipe sumber data?](#) dalam panduan ini.

Jika penilaian Anda dibuat di konsol dari kerangka kerja standar, Audit Manager memilih layanan untuk Anda dan memetakan sumber datanya sesuai dengan persyaratan kerangka kerja. Jika kerangka standar hanya berisi kontrol manual, tidak ada yang Layanan AWS berada dalam cakupan.

 Note

Lain kali Anda mengedit penilaian atau mengubah salah satu kontrol khusus dalam penilaian Anda, Manajer Audit mengambil alih pengelolaan layanan dalam lingkup untuk Anda. Ketika ini terjadi, Layanan AWS tab dihapus dari penilaian Anda.

Tab pemilik audit

Anda dapat menggunakan tab ini untuk melihat pemilik audit untuk penilaian.

Di bagian ini, Anda dapat meninjau informasi berikut:

Nama	Deskripsi
Pemilik audit	Nama pemilik audit.
Akun AWS	Akun AWS ID pemilik audit.

Tab tag

Anda dapat menggunakan tab ini untuk melihat tag penilaian Anda. Tag ini diwarisi dari kerangka kerja yang digunakan untuk membuat penilaian. Untuk informasi selengkapnya tentang tag di Audit Manager, lihat [Sumber daya penandaan AWS Audit Manager](#).

Di bagian ini, Anda dapat meninjau informasi berikut:

Nama	Deskripsi
Kunci	Kunci tag, seperti standar kepatuhan, peraturan, atau kategori.
Nilai	Nilai tag.

Tab Changelog

Anda dapat menggunakan tab ini untuk melihat aktivitas pengguna untuk penilaian.

Di bagian ini, Anda dapat meninjau informasi berikut:

Nama	Deskripsi
Tanggal	Tanggal kegiatan.
Pengguna	Pengguna yang melakukan tindakan.
Tindakan	Tindakan yang terjadi, seperti penilaian yang sedang dibuat.
Jenis	Jenis objek yang berubah, seperti penilaian.
Sumber Daya	Sumber daya yang dipengaruhi oleh perubahan, seperti kerangka kerja tempat penilaian dibuat.

Langkah selanjutnya

Untuk terus meninjau konten penilaian Anda, ikuti langkah-langkah di [Meninjau kontrol penilaian di AWS Audit Manager](#). Halaman ini akan memandu Anda melalui detail kontrol penilaian dan menjelaskan informasi yang Anda lihat di sana.

Sumber daya tambahan

- [Di halaman detail penilaian saya, saya diminta untuk membuat ulang penilaian saya](#)
- [Saya tidak dapat melihat kontrol atau kumpulan kontrol apa pun dalam penilaian saya](#)
- [Saya tidak dapat melihat layanan dalam lingkup penilaian saya](#)

Meninjau kontrol penilaian di AWS Audit Manager

Ketika Anda perlu meninjau kontrol dalam penilaian, Anda akan menemukan informasi yang diatur ke dalam beberapa bagian di halaman detail kontrol penilaian. Bagian ini membantu Anda dengan mudah mengakses dan memahami informasi yang relevan untuk tugas Anda.

Daftar Isi

- [Prasyarat](#)
- [Prosedur](#)
 - [Bagian detail kontrol](#)
 - [Tab Folder Bukti](#)

- [Tab rincian](#)
- [Tab sumber bukti](#)
- [Tab Komentar](#)
- [Tab Changelog](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Prasyarat

Prosedur berikut mengasumsikan bahwa Anda sebelumnya telah membuat setidaknya satu penilaian. Jika Anda belum membuat penilaian, Anda tidak akan melihat hasil apa pun saat mengikuti langkah-langkah ini.

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk melihat penilaian di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Untuk membuka dan meninjau halaman detail kontrol penilaian

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi, pilih **Penilaian** dan pilih nama penilaian untuk membukanya.
3. Dari halaman penilaian, pilih tab **Kontrol**, gulir ke bawah ke tabel **Kumpulan kontrol**, lalu pilih nama kontrol untuk membukanya.
4. Tinjau detail kontrol penilaian menggunakan informasi berikut sebagai referensi.

Bagian dari halaman detail kontrol penilaian

- [Bagian detail kontrol](#)
- [Tab Folder Bukti](#)
- [Tab rincian](#)
- [Tab sumber bukti](#)
- [Tab Komentar](#)

- [Tab Changelog](#)

Bagian detail kontrol

Anda dapat menggunakan bagian Detail kontrol untuk melihat ringkasan kontrol penilaian.

Di bagian ini, Anda dapat meninjau informasi berikut:

Nama	Deskripsi
Deskripsi	Deskripsi yang disediakan untuk kontrol ini.
Status kontrol	Status kontrol. • Sedang ditinjau — Kontrol belum ditinjau. Bukti masih dikumpulkan untuk kontrol ini, dan Anda dapat menambahkan bukti manual. Ini adalah status default. • Ditinjau - Bukti untuk kontrol ini ditinjau. Bukti masih dikumpulkan, dan Anda dapat menambahkan bukti manual. • Tidak aktif — Pengumpulan bukti otomatis dihentikan untuk kontrol ini. Anda tidak dapat lagi menambahkan bukti manual.

Tab Folder Bukti

Anda dapat menggunakan tab ini untuk melihat bukti yang dikumpulkan untuk kontrol ini. Ini diatur ke dalam folder setiap hari. Dari sini, Anda juga dapat mengambil tindakan berikut:

- Tinjau folder bukti — Untuk melihat detail folder bukti apa pun, pilih nama folder yang ditautkan.
- Tambahkan folder bukti ke laporan penilaian — Untuk menyertakan folder bukti, pilih folder tersebut dan pilih Tambahkan ke laporan penilaian.
- Menghapus folder bukti dari laporan penilaian — Untuk mengecualikan folder, pilih folder tersebut dan pilih Hapus dari laporan penilaian.
- Tambahkan bukti manual — Untuk instruksi, lihat [Menambahkan bukti manual di AWS Audit Manager](#).

Di bagian ini, Anda dapat meninjau informasi berikut:

Nama	Deskripsi
Folder bukti	Nama folder bukti. Nama didasarkan pada tanggal ketika bukti dikumpulkan atau ditambahkan secara manual.
Pemeriksaan kepatuhan	Jumlah masalah dalam folder bukti. Angka ini mewakili jumlah total masalah keamanan yang dilaporkan langsung dari AWS Security Hub CSPM, AWS Config, atau keduanya. Jika Anda melihat Tidak berlaku, ini menunjukkan bahwa Anda tidak memiliki CSPM Hub Keamanan atau AWS Config diaktifkan, atau bukti berasal dari jenis sumber data yang berbeda.
Bukti total	Jumlah total item bukti di dalam folder.
Pemilihan laporan penilaian	Jumlah item bukti dalam folder yang disertakan dalam laporan penilaian.

 Tip

Jika Anda tidak dapat melihat folder bukti yang Anda cari, ubah filter dropdown ke Sepanjang waktu. Jika tidak, Anda akan melihat folder tujuh hari terakhir secara default.

Tab rincian

Di bagian ini, Anda dapat meninjau informasi berikut:

Nama	Deskripsi
Informasi pengujian	Prosedur yang disarankan untuk menguji bahwa kontrol berfungsi sebagaimana dimaksud.
Rencana aksi	Tindakan yang disarankan untuk diambil jika kontrol perlu diperbaiki.

Tab sumber bukti

Anda dapat menggunakan tab ini untuk melihat dari mana kontrol penilaian mengumpulkan bukti. Sumber bukti dapat mencakup salah satu dari berikut ini:

Nama	Deskripsi
Kontrol umum	Ini adalah kontrol umum yang mengumpulkan bukti untuk mendukung kontrol penilaian. Kontrol umum mengumpulkan bukti menggunakan sumber data mendasar yang AWS dikelola untuk Anda. Untuk setiap kontrol umum yang terdaftar, Manajer Audit mengumpulkan bukti yang relevan untuk semua kontrol inti pendukung. Pilih kontrol umum untuk melihat kontrol inti terkait.
Kontrol inti	Ini adalah kontrol inti yang mengumpulkan bukti untuk mendukung kontrol penilaian. Kontrol inti mengumpulkan bukti dengan menggunakan kelompok sumber data yang telah ditentukan yang dikelola AWS untuk Anda. Pilih kontrol inti untuk melihat sumber data yang mendasarinya.
Sumber data	Ini adalah sumber data individu yang mengumpulkan bukti untuk mendukung kontrol penilaian. • Nama — Nama sumber data. • Jenis — Jenis sumber data dari mana bukti berasal. • Jika Audit Manager mengumpulkan bukti, jenisnya bisa berupa AWS Security Hub CSPM, AWS Config, AWS CloudTrail, atau panggilan AWS API. • Jika Anda mengunggah bukti Anda sendiri, jenisnya adalah Manual. Deskripsi menunjukkan apakah bukti manual yang diperlukan adalah unggahan File atau respons Teks. • Pemetaan — Kata kunci spesifik yang digunakan untuk mengumpulkan bukti. • Jika jenisnya AWS Config, pemetaan adalah AWS Config aturan (seperti <code>SNS_ENCRYPTED_KMS</code>)

Nama	Deskripsi
	• Jika jenisnya AWS Security Hub CSPM, pemetaan adalah kontrol CSPM Hub Keamanan (seperti <code>EC2.1</code>). • Jika jenisnya adalah panggilan AWS API, pemetaan adalah panggilan API (seperti <code>kms_ListKeys</code>). • Jika jenisnya AWS CloudTrail, pemetaan adalah CloudTrail peristiwa (seperti <code>CreateAccessKey</code>). • Frekuensi — Seberapa sering Audit Manager mengumpulkan bukti untuk sumber data panggilan AWS API.

Tab Komentar

Di tab ini, Anda dapat menambahkan komentar tentang kontrol dan buktinya. Anda juga dapat melihat daftar komentar sebelumnya.

- Di bawah Kirim komentar, Anda dapat menambahkan komentar untuk kontrol dengan memasukkan teks lalu memilih Kirim komentar.
- Di bawah Komentar sebelumnya, Anda dapat melihat daftar komentar sebelumnya bersama dengan tanggal komentar dibuat dan ID pengguna terkait.

Tab Changelog

Anda dapat menggunakan tab ini untuk melihat aktivitas pengguna untuk kontrol penilaian. Informasi yang sama tersedia saat log jejak audit AWS CloudTrail. Dengan aktivitas pengguna yang ditangkap langsung di Audit Manager, Anda dapat dengan mudah meninjau jejak audit aktivitas untuk kontrol yang diberikan.

Di bagian ini, Anda dapat meninjau informasi berikut:

Nama	Deskripsi
Tanggal	Tanggal dan waktu kegiatan, diwakili dalam Waktu Universal Terkoordinasi (UTC).
Pengguna	Pengguna atau peran yang melakukan aktivitas.

Nama	Deskripsi
Tindakan	Tindakan yang terjadi, seperti penilaian yang sedang dibuat.
Jenis	Jenis objek yang berubah, seperti penilaian.
Sumber Daya	Sumber daya yang dipengaruhi oleh perubahan, seperti kerangka kerja tempat penilaian dibuat.

Audit Manager melacak aktivitas pengguna berikut di log perubahan:

- Membuat penilaian
- Mengedit penilaian
- Menyelesaikan penilaian
- Menghapus penilaian
- Mendelegasikan kumpulan kontrol untuk ditinjau
- Mengirimkan set kontrol yang ditinjau kembali ke pemilik audit
- Mengunggah bukti manual
- Memperbarui status kontrol
- Menghasilkan laporan penilaian

Langkah selanjutnya

Untuk terus meninjau penilaian Anda, ikuti langkah-langkah di [Meninjau folder bukti di AWS Audit Manager](#). Halaman ini akan memandu Anda melalui folder bukti dan menunjukkan kepada Anda cara memahami informasi yang Anda lihat.

Sumber daya tambahan

- [Saya tidak dapat melihat kontrol atau kumpulan kontrol apa pun dalam penilaian saya](#)

Meninjau folder bukti di AWS Audit Manager

Saat penilaian Anda mengumpulkan bukti, Audit Manager mengaturnya ke dalam folder untuk kenyamanan Anda. Ketika Anda perlu meninjau folder bukti, Anda akan menemukan informasi yang diatur dalam beberapa bagian.

Daftar Isi

- [Prasyarat](#)
- [Prosedur](#)
 - [Ringkasan folder bukti](#)
 - [Tabel bukti](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Prasyarat

Prosedur berikut mengasumsikan bahwa Anda sebelumnya telah membuat setidaknya satu penilaian. Jika Anda belum membuat penilaian, Anda tidak akan melihat hasil apa pun saat mengikuti langkah-langkah ini.

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk melihat penilaian di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Perlu diingat bahwa diperlukan waktu hingga 24 jam untuk penilaian untuk mulai mengumpulkan bukti otomatis. Jika penilaian Anda belum memiliki bukti, Anda tidak akan melihat hasil apa pun ketika Anda mengikuti langkah-langkah ini.

Prosedur

Untuk membuka dan meninjau folder bukti

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi, pilih Penilaian, lalu pilih penilaian.
3. Dari halaman penilaian, pilih tab Kontrol, gulir ke bawah ke tabel Kontrol, lalu pilih kontrol penilaian.
4. Dari halaman kontrol penilaian, pilih tab Folder Bukti.

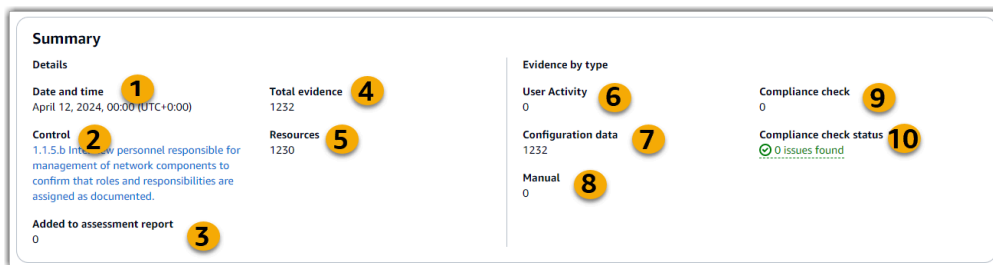
5. Di tabel Folder Bukti, pilih nama folder bukti.
6. Tinjau folder bukti menggunakan informasi berikut sebagai referensi.

Bagian dari halaman folder bukti

- [Ringkasan folder bukti](#)
- [Tabel bukti](#)

Ringkasan folder bukti

Anda dapat menggunakan bagian Ringkasan halaman untuk melihat ikhtisar tingkat tinggi dari bukti di folder bukti. Untuk mempelajari lebih lanjut tentang berbagai jenis bukti, lihat [Bukti](#).



Di bagian ini, Anda dapat meninjau informasi berikut:

Nama	Deskripsi
1. Tanggal dan waktu	Waktu dan tanggal ketika folder bukti dibuat. Ini diwakili dalam Waktu Universal Terkoordinasi (UTC).
2. Kontrol	Nama kontrol yang terkait dengan folder bukti.
3. Ditambahkan ke laporan penilaian	Jumlah item bukti yang dipilih untuk dimasukkan dalam laporan penilaian.
4. Bukti total	Jumlah total item bukti dalam folder bukti.
5. Sumber daya	Jumlah total sumber AWS daya yang dinilai saat mengumpulkan bukti dalam folder ini.
6. Aktivitas pengguna	Jumlah item bukti yang termasuk dalam kategori aktivitas pengguna. Bukti ini dikumpulkan dari AWS CloudTrail log.

Nama	Deskripsi
7. Data konfigurasi	Jumlah item bukti yang termasuk dalam kategori data konfigurasi. Bukti ini dikumpulkan dari panggilan API yang mengambil snapshot konfigurasi lainnya Layanan AWS.
8. Manual	Jumlah item bukti yang termasuk dalam kategori manual. Bukti ini ditambahkan secara manual.
9. Pemeriksaan kepatuhan	Jumlah item bukti yang termasuk dalam kategori pemeriksaan kepatuhan. Bukti ini dikumpulkan dari AWS Config, AWS Security Hub CSPM, atau keduanya.
10. Status pemeriksaan kepatuhan	Jumlah total masalah yang dilaporkan langsung dari AWS Security Hub CSPM, AWS Config, atau keduanya.

Tabel bukti

Anda dapat menggunakan tabel Bukti untuk melihat bukti yang terkandung dalam folder bukti. Dari tabel di sini, Anda juga dapat mengambil tindakan berikut:

- Tinjau bukti individu — Untuk melihat detail bukti apa pun, pilih nama bukti yang ditautkan di bawah kolom Waktu.
- Tambahkan bukti ke laporan penilaian — Untuk menyertakan bukti, pilih dan pilih Tambahkan ke laporan penilaian.
- Menghapus bukti dari laporan penilaian — Untuk mengecualikan bukti, pilih dan pilih Hapus dari laporan penilaian.
- Tambahkan bukti manual — Untuk instruksi, lihat [Menambahkan bukti manual di AWS Audit Manager](#).

Dalam tabel ini, Anda dapat meninjau informasi berikut:

Nama	Deskripsi
Waktu	Menentukan kapan bukti dikumpulkan. Ini juga berfungsi sebagai nama bukti. Waktu diwakili dalam Waktu Universal Terkoordinasi (UTC).
Pemeriksaan kepatuhan	Status evaluasi untuk bukti yang termasuk dalam kategori pemeriksaan kepatuhan. • Untuk bukti yang dikumpulkan dari Security Hub CSPM, hasil Lulus atau Gagal dilaporkan langsung dari Security Hub CSPM. • Untuk bukti yang dikumpulkan dari AWS Config, Putih atau Non-compliant hasil dilaporkan langsung dari AWS Config. • Jika Tidak berlaku ditampilkan, ini menunjukkan bahwa Anda tidak mengaktifkan AWS Config atau CSPM Hub Keamanan, atau bukti berasal dari jenis sumber data yang berbeda.
Bukti berdasarkan jenis	Jenis bukti. • Bukti pemeriksaan kepatuhan dikumpulkan dari AWS Config atau AWS Security Hub CSPM. • Bukti aktivitas pengguna dikumpulkan dari AWS CloudTrail. • Bukti data konfigurasi dikumpulkan dari panggilan API ke yang lain Layanan AWS. • Bukti manual adalah bukti yang Anda tambahkan secara manual.
Sumber data	Sumber data dari mana bukti dikumpulkan.
Nama acara	Nama acara yang meminta pengumpulan bukti.
Sumber acara	Prinsip layanan yang mengidentifikasi yang relevan Layanan AWS untuk acara tersebut.
Sumber daya	Jumlah sumber daya yang dinilai saat mengumpulkan bukti.
Pemilihan laporan penilaian	Menunjukkan apakah bukti termasuk dalam laporan penilaian.

Nama	Deskripsi
	• Untuk memasukkan bukti, pilih bukti dan pilih Tambahkan ke laporan penilaian. • Untuk mengecualikan bukti, pilih bukti dan pilih Hapus dari laporan penilaian.

Langkah selanjutnya

Saat Anda siap untuk menjelajahi setiap bukti dalam folder, ikuti langkah-langkah di [Meninjau bukti di AWS Audit Manager](#). Halaman ini akan memandu Anda melalui detail bukti dan cara menafsirkan informasi yang Anda lihat di sana.

Sumber daya tambahan

- Untuk solusi untuk masalah bukti di Manajer Audit, lihat [Memecahkan masalah penilaian dan pengumpulan bukti](#).

Meninjau bukti di AWS Audit Manager

Ketika Anda perlu meninjau bukti tertentu, ikuti instruksi di halaman ini. Anda akan menemukan detail bukti yang disusun menjadi beberapa bagian.

Daftar Isi

- [Prasyarat](#)
- [Prosedur](#)
 - [Ringkasan](#)
 - [Atribut](#)
 - [Sumber daya termasuk](#)
- [Sumber daya tambahan](#)

Prasyarat

Prosedur berikut mengasumsikan bahwa Anda sebelumnya telah membuat setidaknya satu penilaian. Jika Anda belum membuat penilaian, Anda tidak akan melihat hasil apa pun saat mengikuti langkah-langkah ini.

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk melihat penilaian di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Perlu diingat bahwa diperlukan waktu hingga 24 jam untuk penilaian untuk mulai mengumpulkan bukti otomatis. Jika penilaian Anda belum memiliki bukti, Anda tidak akan melihat hasil apa pun ketika Anda mengikuti langkah-langkah ini.

Prosedur

Untuk membuka dan meninjau halaman detail bukti

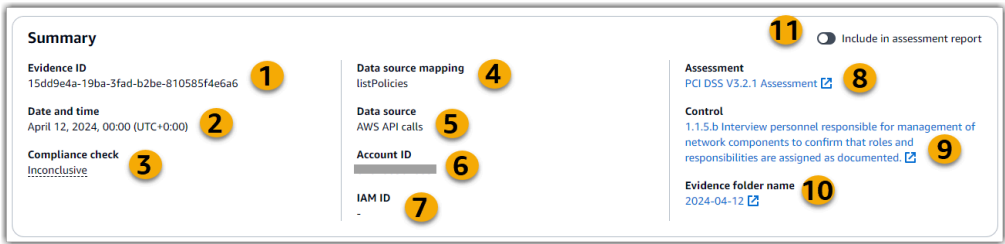
1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi, pilih Penilaian, lalu pilih penilaian.
3. Dari halaman penilaian, pilih tab Kontrol, gulir ke bawah ke tabel Kontrol, lalu pilih kontrol.
4. Dari halaman kontrol, pilih tab Folder Bukti.
5. Di tabel Folder Bukti, pilih nama folder bukti.
6. Pilih nama bukti di bawah kolom Waktu untuk membuka halaman detail bukti.
7. Tinjau detail bukti menggunakan informasi berikut sebagai referensi.

Bagian dari halaman detail bukti

- [Ringkasan](#)
- [Atribut](#)
- [Sumber daya termasuk](#)

Ringkasan

Anda dapat menggunakan bagian Ringkasan untuk melihat ikhtisar bukti.



Di bagian ini, Anda dapat meninjau informasi berikut:

Nama	Deskripsi
1. ID Bukti	Pengidentifikasi unik untuk bukti.
2. Tanggal dan waktu	Waktu dan tanggal ketika bukti dikumpulkan. Ini diwakili dalam Waktu Universal Terkoordinasi (UTC).
3. Pemeriksaan kepatuhan	Status evaluasi untuk bukti pemeriksaan kepatuhan. • Untuk bukti yang dikumpulkan dari AWS Security Hub CSPM, hasil Lulus atau Gagal dilaporkan langsung dari AWS Security Hub CSPM. • Untuk bukti yang dikumpulkan dari AWS Config, Patuh atau Non-compliant hasil dilaporkan langsung dari AWS Config. • Jika Tidak berlaku ditampilkan, ini menunjukkan salah satu dari dua hal. Entah Anda tidak memiliki AWS Security Hub CSPM atau AWS Config mengaktifkan. Atau, bukti berasal dari sumber data yang berbeda.
4. Pemetaan sumber data	Kata kunci pemetaan yang digunakan untuk mengumpulkan bukti.
5. Jenis sumber data	Jenis sumber data tempat bukti dikumpulkan.
6. ID Akun	Akun AWS Itu terkait dengan bukti.
7. ID IAM	Pengguna atau peran yang relevan, jika berlaku.
8. Penilaian	Nama penilaian yang terkait dengan bukti.
9. Kontrol	Nama kontrol yang terkait dengan bukti.

Nama	Deskripsi
10. Nama folder bukti	Nama folder bukti yang berisi bukti.
11. Termasuk dalam laporan penilaian	Sakelar yang memungkinkan Anda untuk memasukkan atau mengecualikan bukti dari laporan penilaian.

Atribut

Anda dapat menggunakan tabel Atribut untuk melihat atribut bukti secara detail.

Dalam tabel ini, Anda dapat meninjau informasi berikut:

Nama	Deskripsi
Nama atribut	Kunci untuk atribut.
Nilai	Nilai atribut. Dalam beberapa kasus, tautan ke file JSON disediakan dengan informasi lebih lanjut.

Sumber daya termasuk

Anda dapat menggunakan tabel Sumber daya yang disertakan untuk melihat sumber daya yang dinilai untuk menghasilkan bukti ini.

Di bagian ini, Anda dapat meninjau informasi berikut:

Nama	Deskripsi
ARN	Amazon Resource Name (ARN) dari sumber daya. ARN mungkin tidak tersedia untuk semua jenis bukti.
Kepatuhan sumber daya	Status evaluasi untuk sumber daya. Untuk bukti yang dikumpulkan dari AWS Security Hub CSPM, hasil Lulus atau Gagal dilaporkan langsung dari Security Hub CSPM.

Nama	Deskripsi
	• Untuk bukti yang dikumpulkan dari AWS Config, P atuh atau Non-compliant hasil dilaporkan langsung dari AWS Config. • Jika Tidak berlaku ditampilkan, ini menunjukkan bahwa Anda tidak mengaktifkan AWS Config atau CSPM Hub Keamanan, atau bukti berasal dari sumber data yang berbeda.
Nilai	Informasi lebih lanjut tentang penilaian sumber daya. Dalam beberapa kasus, tautan ke file JSON disediakan dengan informasi lebih lanjut.

Sumber daya tambahan

- Untuk solusi untuk masalah bukti di Manajer Audit, lihat [Memecahkan masalah penilaian dan pengumpulan bukti](#).

Mengedit penilaian di AWS Audit Manager

Anda mungkin menghadapi situasi di mana Anda perlu mengedit penilaian yang ada AWS Audit Manager. Mungkin ruang lingkup audit Anda telah berubah, memerlukan pembaruan untuk yang Akun AWS disertakan dalam penilaian. Atau, Anda mungkin perlu merevisi daftar pemilik audit yang ditugaskan untuk penilaian karena perubahan personel. Dalam kasus seperti itu, Anda dapat mengedit penilaian aktif Anda dan membuat penyesuaian yang diperlukan tanpa mengganggu pengumpulan bukti Anda.

Halaman berikut menguraikan langkah-langkah untuk mengedit detail penilaian Anda, mengubah cakupan Akun AWS, memperbarui pemilik audit, dan meninjau serta menyimpan perubahan Anda.

Prasyarat

Prosedur berikut mengasumsikan bahwa Anda sebelumnya telah membuat setidaknya satu penilaian, dan itu dalam keadaan aktif.

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk mengedit penilaian di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah

[AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Tugas

- [Langkah 1: Edit detail penilaian](#)
- [Langkah 2: Sunting Akun AWS dalam ruang lingkup](#)
- [Langkah 3: Edit pemilik audit](#)
 - [Izin pemilik audit](#)
- [Langkah 4: Tinjau dan simpan](#)

Langkah 1: Edit detail penilaian

Ikuti langkah-langkah ini untuk mengedit detail penilaian Anda.

Untuk mengedit penilaian

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi, pilih **Assessments**.
3. Pilih penilaian, dan pilih **Edit**.
4. Di bawah **Edit detail penilaian**, edit detail penilaian Anda sesuai kebutuhan.
5. Pilih **Berikutnya**.

Langkah 2: Sunting Akun AWS dalam ruang lingkup

Pada langkah ini, Anda dapat mengubah akun mana yang disertakan dalam penilaian Anda. Audit Manager dapat mendukung hingga 200 akun dalam lingkup penilaian, dan 250 akun anggota unik di semua penilaian.

Untuk mengedit Akun AWS dalam ruang lingkup

1. Untuk menambahkan Akun AWS, pilih kotak centang di sebelah nama akun.
2. Untuk menghapus Akun AWS, kosongkan kotak centang di sebelah nama akun.
3. Pilih **Berikutnya**.

Note

Untuk mengedit administrator yang didelegasikan untuk Audit Manager, lihat [Mengubah administrator yang didelegasikan](#).

Langkah 3: Edit pemilik audit

Pada langkah ini, Anda dapat mengubah pemilik audit yang disertakan dalam penilaian Anda.

Untuk mengedit pemilik audit

1. Untuk menambahkan pemilik audit, pilih kotak centang di sebelah nama akun.
2. Untuk menghapus pemilik audit, kosongkan kotak centang di samping nama akun.
3. Pilih Berikutnya.

Izin pemilik audit

Kebijakan di bawah ini dilampirkan untuk semua pemilik audit penilaian.

Audit Manager menggantinya *placeholder text* dengan pengidentifikasi akun dan sumber daya Anda sebelum melampirkan kebijakan.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AuditOwner",
      "Effect": "Allow",
      "Principal": {
        "AWS": "Principal for user/role who are the audit owners of the Assessment"
      },
      "Action": [
        "auditmanager:GetAssessment",
        "auditmanager:UpdateAssessment",
        "auditmanager:UpdateAssessmentControlSetStatus",
        "auditmanager:UpdateAssessmentStatus",

```



```

        "auditmanager:UpdateAssessmentControl",
        "auditmanager:DeleteAssessment",
        "auditmanager:GetChangeLogs",
        "auditmanager:GetEvidenceFoldersByAssessment",
        "auditmanager:GetEvidenceFoldersByAssessmentControl",
        "auditmanager:BatchImportEvidenceToAssessmentControl",
        "auditmanager:GetEvidenceFolder",
        "auditmanager:GetEvidence",
        "auditmanager:GetEvidenceByEvidenceFolder",
        "auditmanager:BatchCreateDelegationByAssessment",
        "auditmanager:BatchDeleteDelegationByAssessment",
        "auditmanager:AssociateAssessmentReportEvidenceFolder",
        "auditmanager:BatchAssociateAssessmentReportEvidence",
        "auditmanager:BatchDisassociateAssessmentReportEvidence",
        "auditmanager:CreateAssessmentReport",
        "auditmanager:DeleteAssessmentReport",
        "auditmanager:DisassociateAssessmentReportEvidenceFolder",
        "auditmanager:GetAssessmentReportUrl"
    ],
    "Resource": [
        "arn:aws:auditmanager:us-  

east-1:123456789012:assessment/assessment_ID",
        "arn:aws:auditmanager:us-  

east-1:123456789012:assessment/assessment_ID/*"
    ]
}
]
}

```

Langkah 4: Tinjau dan simpan

Tinjau informasi untuk penilaian Anda. Untuk mengubah informasi untuk satu langkah, pilih **Edit**. Setelah selesai, pilih **Simpan perubahan** untuk mengonfirmasi pengeditan Anda.

Setelah Anda menyelesaikan pengeditan, perubahan penilaian akan berlaku pada pukul 00:00 UTC pada hari berikutnya.

Langkah selanjutnya

Ketika Anda tidak perlu lagi mengumpulkan bukti untuk kontrol penilaian tertentu, Anda dapat mengubah status kontrol itu. Untuk petunjuk, lihat [Mengubah status kontrol penilaian di AWS Audit Manager](#).

Ketika Anda tidak perlu lagi mengumpulkan bukti untuk seluruh penilaian, Anda dapat mengubah status penilaian menjadi tidak aktif. Untuk petunjuk, lihat [Mengubah status penilaian menjadi tidak aktif di AWS Audit Manager](#).

Sumber daya tambahan

- Untuk solusi untuk masalah penilaian di Manajer Audit, lihat [Memecahkan masalah penilaian dan pengumpulan bukti](#).
- Untuk informasi tentang mengapa tidak mungkin lagi mengedit layanan dalam cakupan, lihat [Saya tidak dapat mengedit layanan dalam lingkup penilaian saya](#) di bagian Pemecahan Masalah pada panduan ini.

Menambahkan bukti manual di AWS Audit Manager

Manajer Audit dapat secara otomatis mengumpulkan bukti untuk banyak kontrol. Namun, beberapa kontrol mungkin memerlukan bukti yang tidak dapat dikumpulkan secara otomatis. Dalam kasus seperti itu, Anda dapat menambahkan bukti Anda sendiri secara manual.

Pertimbangkan contoh berikut:

- Beberapa kontrol berhubungan dengan penyediaan catatan fisik (seperti tanda tangan), atau peristiwa yang tidak dihasilkan di cloud (seperti pengamatan dan wawancara). Dalam kasus ini, Anda dapat menambahkan file secara manual sebagai bukti. Misalnya, jika kontrol memerlukan informasi tentang struktur organisasi Anda, Anda dapat mengunggah salinan bagan organisasi perusahaan Anda sebagai bukti manual.
- Beberapa kontrol mewakili pertanyaan penilaian risiko vendor. Pertanyaan penilaian risiko mungkin memerlukan dokumentasi sebagai bukti (seperti bagan organisasi). Atau, mungkin hanya membutuhkan respons teks sederhana (seperti daftar judul pekerjaan). Untuk yang terakhir, Anda dapat menanggapi pertanyaan dan menyimpan tanggapan Anda sebagai bukti manual.

Anda juga dapat menggunakan fitur unggahan manual untuk mengelola bukti dari berbagai lingkungan. Jika perusahaan Anda menggunakan model cloud hybrid atau model multicloud, Anda dapat mengunggah bukti dari lingkungan lokal, lingkungan yang dihosting di cloud, atau aplikasi SaaS Anda. Ini memungkinkan Anda untuk mengatur bukti Anda (terlepas dari mana asalnya) dengan menyimpannya dalam struktur penilaian Manajer Audit, di mana setiap bukti dipetakan ke kontrol tertentu.

Poin kunci

Ketika harus menambahkan bukti manual ke penilaian Anda di Audit Manager, Anda memiliki tiga metode untuk dipilih.

1. Mengimpor file dari Amazon S3 - Metode ini sangat ideal jika Anda memiliki file bukti yang disimpan dalam bucket S3, seperti dokumentasi, laporan, atau artefak lain yang tidak dapat dikumpulkan secara otomatis oleh Audit Manager. Dengan mengimpor file-file ini langsung dari S3, Anda dapat dengan mulus mengintegrasikan bukti manual ini dengan bukti yang dikumpulkan secara otomatis.
2. Mengunggah file dari browser Anda - Jika Anda memiliki file bukti yang disimpan secara lokal di komputer atau jaringan Anda, Anda dapat mengunggahnya secara manual ke Audit Manager menggunakan metode ini. Pendekatan ini sangat berguna ketika Anda perlu menyertakan catatan fisik, seperti dokumen atau gambar yang dipindai, yang tidak tersedia dalam format digital di AWS lingkungan Anda.
3. Menambahkan teks bentuk bebas sebagai bukti - Dalam beberapa kasus, bukti yang perlu Anda berikan bukan dalam bentuk file melainkan tanggapan teks atau penjelasan. Metode ini memungkinkan Anda untuk memasukkan teks bentuk bebas langsung ke Audit Manager. Ini dapat sangat membantu ketika menanggapi pertanyaan penilaian risiko vendor.

Sumber daya tambahan

- Untuk petunjuk tentang cara menambahkan bukti manual ke kontrol penilaian, lihat sumber daya berikut. Ingatlah bahwa Anda hanya dapat menggunakan satu metode pada satu waktu.
 - [Mengimpor file bukti manual dari Amazon S3](#)
 - [Mengunggah file bukti manual dari browser Anda](#)
 - [Memasukkan tanggapan teks bentuk bebas sebagai bukti manual](#)
- Untuk mempelajari format file mana yang dapat Anda gunakan, lihat [Format file yang didukung untuk bukti manual](#).
- Untuk mempelajari lebih lanjut tentang berbagai jenis bukti di Audit Manager, lihat [evidence](#) di bagian Konsep dan terminologi panduan ini.
- Untuk bantuan pemecahan masalah, lihat [Saya tidak dapat mengunggah bukti manual ke kontrol](#).

Mengimpor file bukti manual dari Amazon S3

Anda dapat mengimpor file bukti secara manual dari bucket Amazon S3 ke dalam penilaian Anda. Ini memungkinkan Anda untuk melengkapi bukti yang dikumpulkan secara otomatis dengan bahan pendukung tambahan.

Prasyarat

- Ukuran maksimum yang didukung untuk satu file bukti manual adalah 100 MB.
- Anda harus menggunakan salah satunya [Format file yang didukung untuk bukti manual](#).
- Masing-masing Akun AWS dapat secara manual mengunggah hingga 100 file bukti ke kontrol setiap hari. Melebihi kuota harian ini menyebabkan unggahan manual tambahan gagal untuk kontrol tersebut. Jika Anda perlu mengunggah sejumlah besar bukti manual ke satu kontrol, unggah bukti Anda secara berkelompok selama beberapa hari.
- Ketika kontrol tidak aktif, Anda tidak dapat menambahkan bukti manual ke kontrol itu. Untuk menambahkan bukti manual, Anda harus terlebih [dahulu mengubah status kontrol](#) menjadi sedang ditinjau atau ditinjau.
- Pastikan identitas IAM Anda memiliki izin yang sesuai untuk mengelola penilaian di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Anda dapat mengimpor file menggunakan konsol Audit Manager, API Audit Manager, atau AWS Command Line Interface (AWS CLI).

AWS console

Important

Kami sangat menyarankan agar Anda tidak pernah mengimpor informasi sensitif atau identitas pribadi (PII) sebagai bukti manual. Ini termasuk, tetapi tidak terbatas pada, nomor Jaminan Soal, alamat, nomor telepon, atau informasi lain yang dapat digunakan untuk mengidentifikasi seseorang.

Untuk mengimpor file dari S3 di konsol Audit Manager

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.

2. Di panel navigasi kiri, pilih **Penilaian**, lalu pilih penilaian.
3. Pilih tab **Kontrol**, gulir ke bawah ke **Kumpulan kontrol** dan kemudian pilih kontrol.
4. Pada tab **Folder Bukti**, pilih **Tambahkan bukti manual**, lalu pilih **Impor file dari S3**.
5. Pada halaman berikutnya, masukkan URI S3 bukti. Anda dapat menemukan URI S3 dengan menavigasi ke objek di konsol [Amazon S3](#) dan memilih **Salin URI S3**.
6. Pilih **Unggah**.

AWS CLI

Important

Kami sangat menyarankan agar Anda tidak pernah mengimpor informasi sensitif atau identitas pribadi (PII) sebagai bukti manual. Ini termasuk, tetapi tidak terbatas pada, nomor Jaminan Soal, alamat, nomor telepon, atau informasi lain yang dapat digunakan untuk mengidentifikasi seseorang.

Dalam prosedur berikut, ganti *placeholder text* dengan informasi Anda sendiri.

Untuk mengimpor file dari S3 di AWS CLI

1. Jalankan [list-assessments](#) kan perintah untuk melihat daftar penilaian Anda.

```
aws auditmanager list-assessments
```

Dalam tanggapan, temukan penilaian yang ingin Anda unggah bukti dan catat ID penilaian.

2. Jalankan [get-assessment](#) kan perintah dan tentukan ID penilaian dari langkah satu.

```
aws auditmanager get-assessment --assessment-id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

Dalam tanggapan, temukan kumpulan kontrol dan kontrol yang ingin Anda unggah bukti, dan catat ID-nya.

3. Jalankan [batch-import-evidence-to-assessment-control](#) kan perintah dengan parameter berikut:

- `--assessment-id`—Gunakan ID penilaian dari langkah satu.

- `--control-set-id`— Gunakan ID set kontrol dari langkah dua.
- `--control-id`— Gunakan ID kontrol dari langkah kedua.
- `--manual-evidence`— Gunakan `s3ResourcePath` sebagai jenis bukti manual dan tentukan URI S3 bukti. Anda dapat menemukan URI S3 dengan menavigasi ke objek di konsol [Amazon S3](#) dan memilih Salin URI S3.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence s3ResourcePath=s3://amzn-s3-demo-bucket/EXAMPLE-FILE.extension
```

Audit Manager API

Important

Kami sangat menyarankan agar Anda tidak pernah mengimpor informasi sensitif atau identitas pribadi (PII) sebagai bukti manual. Ini termasuk, tetapi tidak terbatas pada, nomor Jaminan Soal, alamat, nomor telepon, atau informasi lain yang dapat digunakan untuk mengidentifikasi seseorang.

Untuk mengimpor file dari S3 menggunakan API

1. Hubun [ListAssessments](#) gi operasi untuk melihat daftar penilaian Anda. Dalam tanggapan, temukan penilaian yang ingin Anda unggah bukti dan catat ID penilaian.
2. Panggil [GetAssessment](#) operasi dan tentukan ID penilaian dari langkah satu. Dalam tanggapan, temukan kumpulan kontrol dan kontrol yang ingin Anda unggah bukti, dan catat ID-nya.
3. Panggil operasi [BatchImportEvidenceToAssessmentControl](#) dengan parameter berikut ini:
 - [assessmentId](#)— Gunakan ID penilaian dari langkah satu.
 - [controlSetId](#)— Gunakan ID set kontrol dari langkah dua.
 - [controlId](#)— Gunakan ID kontrol dari langkah kedua.

- [manualEvidence](#)— Gunakan `s3ResourcePath` sebagai jenis bukti manual dan tentukan URI S3 bukti. Anda dapat menemukan URI S3 dengan menavigasi ke objek di konsol [Amazon S3](#) dan memilih Salin URI S3.

Untuk informasi selengkapnya, pilih salah satu tautan dalam prosedur sebelumnya untuk membaca lebih lanjut di Refer AWS Audit Manager ensi API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasa AWS .

Langkah selanjutnya

Setelah Anda menambahkan dan meninjau bukti untuk penilaian Anda, Anda dapat membuat laporan penilaian. Untuk informasi selengkapnya, lihat [Menyiapkan laporan penilaian di AWS Audit Manager](#).

Sumber daya tambahan

Untuk mempelajari format file mana yang dapat Anda gunakan, lihat [Format file yang didukung untuk bukti manual](#).

Mengunggah file bukti manual dari browser Anda

Anda dapat mengunggah file bukti secara manual dari browser Anda ke penilaian Manajer Audit Anda. Ini memungkinkan Anda untuk melengkapi bukti yang dikumpulkan secara otomatis dengan bahan pendukung tambahan.

Prasyarat

- Ukuran maksimum yang didukung untuk satu file bukti manual adalah 100 MB.
- Anda harus menggunakan salah satunya [Format file yang didukung untuk bukti manual](#).
- Masing-masing Akun AWS dapat secara manual mengunggah hingga 100 file bukti ke kontrol setiap hari. Melebihi kuota harian ini menyebabkan unggahan manual tambahan gagal untuk kontrol tersebut. Jika Anda perlu mengunggah sejumlah besar bukti manual ke satu kontrol, unggah bukti Anda secara berkelompok selama beberapa hari.
- Ketika kontrol tidak aktif, Anda tidak dapat menambahkan bukti manual ke kontrol itu. Untuk menambahkan bukti manual, Anda harus terlebih [dahulu mengubah status kontrol](#) menjadi sedang ditinjau atau ditinjau.

- Pastikan identitas IAM Anda memiliki izin yang sesuai untuk mengelola penilaian di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Anda dapat mengunggah file menggunakan konsol Audit Manager, API Manajer Audit, atau AWS Command Line Interface (AWS CLI).

AWS console

Important

Kami sangat menyarankan agar Anda tidak pernah mengunggah informasi sensitif atau identitas pribadi (PII) sebagai bukti manual. Ini termasuk, tetapi tidak terbatas pada, nomor Jaminan Soal, alamat, nomor telepon, atau informasi lain yang dapat digunakan untuk mengidentifikasi seseorang.

Untuk mengunggah file dari browser Anda di konsol Audit Manager

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi kiri, pilih Penilaian, lalu pilih penilaian.
3. Pada tab Kontrol, gulir ke bawah ke Kumpulan kontrol dan kemudian pilih kontrol.
4. Dari tab Folder Bukti, pilih Tambahkan bukti manual.
5. Pilih Unggah file dari browser.
6. Pilih file yang ingin Anda unggah.
7. Pilih Unggah.

AWS CLI

Important

Kami sangat menyarankan agar Anda tidak pernah mengunggah informasi sensitif atau identitas pribadi (PII) sebagai bukti manual. Ini termasuk, tetapi tidak terbatas pada,

nomor Jaminan Soal, alamat, nomor telepon, atau informasi lain yang dapat digunakan untuk mengidentifikasi seseorang.

Dalam prosedur berikut, ganti *placeholder text* dengan informasi Anda sendiri.

Untuk mengunggah file dari browser Anda di AWS CLI

1. Jalan [list-assessments](#) kan perintah untuk melihat daftar penilaian Anda.

```
aws auditmanager list-assessments
```

Dalam tanggapan, temukan penilaian yang ingin Anda unggah bukti dan catat ID penilaian.

2. Jalan [get-assessment](#) kan perintah dan tentukan ID penilaian dari langkah satu.

```
aws auditmanager get-assessment --assessment-id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

Dalam tanggapan, temukan kumpulan kontrol dan kontrol yang ingin Anda unggah bukti, dan catat ID-nya.

3. Jalan [get-evidence-file-upload-url](#) kan perintah dan tentukan file yang ingin Anda unggah.

```
aws auditmanager get-evidence-file-upload-url --file-name fileName.extension
```

Dalam tanggapan, perhatikan URL yang telah ditandatangani sebelumnya dan `evidenceFileName`

4. Gunakan URL yang telah ditandatangani sebelumnya dari langkah ketiga untuk mengunggah file dari browser Anda. Tindakan ini mengunggah file Anda ke Amazon S3, di mana file tersebut disimpan sebagai objek yang dapat dilampirkan ke kontrol penilaian. Pada langkah berikut, Anda akan mereferensikan objek yang baru dibuat dengan menggunakan parameter `evidenceFileName`

 Note

Saat Anda mengunggah file menggunakan URL yang telah ditandatangani sebelumnya, Audit Manager melindungi dan menyimpan data Anda dengan

menggunakan enkripsi sisi server dengan AWS Key Management Service. Untuk mendukung ini, Anda harus menggunakan `x-amz-server-side-encryption` header dalam permintaan Anda saat Anda menggunakan URL yang telah ditandatangani sebelumnya untuk mengunggah file Anda.

Jika Anda menggunakan pelanggan yang dikelola AWS KMS key di [Mengkonfigurasi pengaturan enkripsi data Anda](#) setelah Audit Manager, pastikan Anda juga menyertakan `x-amz-server-side-encryption-aws-kms-key-id` header dalam permintaan Anda. Jika `x-amz-server-side-encryption-aws-kms-key-id` header tidak ada dalam permintaan, Amazon S3 mengasumsikan bahwa Anda ingin menggunakan Kunci yang dikelola AWS.

Untuk informasi selengkapnya, lihat [Melindungi data menggunakan enkripsi sisi server dengan AWS Key Management Service kunci \(SSE-KMS\)](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

5. Jalankan [batch-import-evidence-to-assessment-control](#) kan perintah dengan parameter berikut:

- `--assessment-id`—Gunakan ID penilaian dari langkah satu.
- `--control-set-id`—Gunakan ID set kontrol dari langkah dua.
- `--control-id`—Gunakan ID kontrol dari langkah kedua.
- `--manual-evidence`—Gunakan `evidenceFileName` sebagai jenis bukti manual dan tentukan nama file bukti dari langkah ketiga.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence evidenceFileName=fileName.extension
```

Audit Manager API

Important

Kami sangat menyarankan agar Anda tidak pernah mengunggah informasi sensitif atau identitas pribadi (PII) sebagai bukti manual. Ini termasuk, tetapi tidak terbatas pada,

nomor Jaminan Soal, alamat, nomor telepon, atau informasi lain yang dapat digunakan untuk mengidentifikasi seseorang.

Untuk mengunggah file dari browser Anda menggunakan API

1. Panggil [ListAssessments](#) operasi. Dalam tanggapan, temukan penilaian yang ingin Anda unggah bukti dan catat ID penilaian.
2. Panggil [GetAssessment](#) operasi dan tentukan `assessmentId` dari langkah satu. Dalam tanggapan, temukan kumpulan kontrol dan kontrol yang ingin Anda unggah bukti, dan catat ID-nya.
3. Panggil [GetEvidenceFileUploadUrl](#) operasi dan tentukan `fileName` yang ingin Anda unggah. Dalam tanggapan, perhatikan URL yang telah ditandatangani sebelumnya dan `evidenceFileName`.
4. Gunakan URL yang telah ditandatangani sebelumnya dari langkah ketiga untuk mengunggah file dari browser Anda. Tindakan ini mengunggah file Anda ke Amazon S3, di mana file tersebut disimpan sebagai objek yang dapat dilampirkan ke kontrol penilaian. Pada langkah berikut, Anda akan mereferensikan objek yang baru dibuat dengan menggunakan parameter `evidenceFileName`.

 Note

Saat Anda mengunggah file menggunakan URL yang telah ditandatangani sebelumnya, Audit Manager melindungi dan menyimpan data Anda dengan menggunakan enkripsi sisi server dengan AWS Key Management Service. Untuk mendukung ini, Anda harus menggunakan `x-amz-server-side-encryption` header dalam permintaan Anda saat Anda menggunakan URL yang telah ditandatangani sebelumnya untuk mengunggah file Anda.

Jika Anda menggunakan pelanggan yang dikelola AWS KMS key di [Mengkonfigurasi pengaturan enkripsi data Anda](#) setelah Audit Manager, pastikan Anda juga menyertakan `x-amz-server-side-encryption-aws-kms-key-id` header dalam permintaan Anda. Jika `x-amz-server-side-encryption-aws-kms-key-id` header tidak ada dalam permintaan, Amazon S3 mengasumsikan bahwa Anda ingin menggunakan Kunci yang dikelola AWS.

Untuk informasi selengkapnya, lihat [Melindungi data menggunakan enkripsi sisi server dengan AWS Key Management Service kunci \(SSE-KMS\)](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

5. Panggil operasi [BatchImportEvidenceToAssessmentControl](#) dengan parameter berikut ini:
- [assessmentId](#)— Gunakan ID penilaian dari langkah satu.
 - [controlSetId](#)— Gunakan ID set kontrol dari langkah dua.
 - [controlId](#)— Gunakan ID kontrol dari langkah kedua.
 - [manualEvidence](#)— Gunakan `evidenceFileName` sebagai jenis bukti manual dan tentukan nama file bukti dari langkah ketiga.

Untuk informasi selengkapnya, pilih salah satu tautan dalam prosedur sebelumnya untuk membaca lebih lanjut di Refer AWS Audit Manager ensi API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasa AWS .

Langkah selanjutnya

Setelah Anda mengumpulkan dan meninjau bukti untuk penilaian Anda, Anda dapat membuat laporan penilaian. Untuk informasi selengkapnya, lihat [Menyiapkan laporan penilaian di AWS Audit Manager](#).

Sumber daya tambahan

Untuk mempelajari format file mana yang dapat Anda gunakan, lihat [Format file yang didukung untuk bukti manual](#).

Memasukkan tanggapan teks bentuk bebas sebagai bukti manual

Anda dapat memberikan konteks tambahan dan informasi pendukung untuk kontrol penilaian dengan memasukkan teks bentuk bebas dan menyimpan teks itu sebagai bukti. Ini memungkinkan Anda untuk mendokumentasikan detail secara manual yang tidak ditangkap melalui pengumpulan bukti otomatis.

Misalnya, Anda dapat menggunakan Audit Manager untuk membuat kontrol khusus yang mewakili pertanyaan dalam kuesioner penilaian risiko vendor. Dalam hal ini, nama setiap kontrol adalah

pertanyaan spesifik yang meminta informasi tentang postur keamanan dan kepatuhan organisasi Anda. Untuk merekam tanggapan Anda terhadap pertanyaan penilaian risiko vendor tertentu, Anda dapat memasukkan respons teks dan menyimpannya sebagai bukti manual untuk kontrol.

Prasyarat

- Ketika kontrol tidak aktif, Anda tidak dapat menambahkan bukti manual ke kontrol itu. Untuk menambahkan bukti manual, Anda harus terlebih dahulu [dahulu mengubah status kontrol](#) menjadi sedang ditinjau atau ditinjau.
- Pastikan identitas IAM Anda memiliki izin yang sesuai untuk mengelola penilaian di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Anda dapat memasukkan tanggapan teks menggunakan konsol Audit Manager, API Manajer Audit, atau AWS Command Line Interface (AWS CLI).

AWS console

Important

Kami sangat menyarankan agar Anda tidak pernah memasukkan informasi sensitif atau identitas pribadi (PII) sebagai bukti manual. Ini termasuk, tetapi tidak terbatas pada, nomor Jaminan Soal, alamat, nomor telepon, atau informasi lain yang dapat digunakan untuk mengidentifikasi seseorang.

Untuk memasukkan respons teks di konsol Audit Manager

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi kiri, pilih Penilaian, lalu pilih penilaian.
3. Pilih tab Kontrol, gulir ke bawah ke Kumpulan kontrol dan kemudian pilih kontrol.
4. Dari tab Folder Bukti, pilih Tambahkan bukti manual.
5. Pilih Masukkan respons teks.
6. Di jendela pop-up yang muncul, masukkan respons Anda dalam format teks biasa.

7. Pilih Konfirmasi.

AWS CLI

Important

Kami sangat menyarankan agar Anda tidak pernah memasukkan informasi sensitif atau identitas pribadi (PII) sebagai bukti manual. Ini termasuk, tetapi tidak terbatas pada, nomor Jaminan Soal, alamat, nomor telepon, atau informasi lain yang dapat digunakan untuk mengidentifikasi seseorang.

Dalam prosedur berikut, ganti *placeholder text* dengan informasi Anda sendiri.

Untuk memasukkan respons teks di AWS CLI

1. Jalankan perintah [list-assessments](#).

```
aws auditmanager list-assessments
```

Dalam tanggapan, temukan penilaian yang ingin Anda unggah bukti dan catat ID penilaian.

2. Jalankan [get-assessment](#) kan perintah dan tentukan ID penilaian dari langkah satu.

```
aws auditmanager get-assessment --assessment-id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

Dalam tanggapan, temukan kumpulan kontrol dan kontrol yang ingin Anda unggah bukti, dan catat ID-nya.

3. Jalankan [batch-import-evidence-to-assessment-control](#) kan perintah dengan parameter berikut:

- `--assessment-id`—Gunakan ID penilaian dari langkah satu.
- `--control-set-id`—Gunakan ID set kontrol dari langkah dua.
- `--control-id`—Gunakan ID kontrol dari langkah kedua.
- `--manual-evidence`—Gunakan `textResponse` sebagai jenis bukti manual dan masukkan teks yang ingin Anda simpan sebagai bukti manual.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence textResponse="enter text here"
```

Audit Manager API

Important

Kami sangat menyarankan agar Anda tidak pernah memasukkan informasi sensitif atau identitas pribadi (PII) sebagai bukti manual. Ini termasuk, tetapi tidak terbatas pada, nomor Jaminan Soal, alamat, nomor telepon, atau informasi lain yang dapat digunakan untuk mengidentifikasi seseorang.

Untuk memasukkan respons teks menggunakan API

1. Panggil [ListAssessments](#) operasi. Dalam tanggapan, temukan penilaian yang ingin Anda unggah bukti dan catat ID penilaian.
2. Panggil [GetAssessment](#) operasi dan tentukan `assessmentId` dari langkah satu. Dalam tanggapan, temukan kumpulan kontrol dan kontrol yang ingin Anda unggah bukti, dan catat ID-nya.
3. Panggil operasi [BatchImportEvidenceToAssessmentControl](#) dengan parameter berikut ini:
 - [assessmentId](#)— Gunakan ID penilaian dari langkah satu.
 - [controlSetId](#)— Gunakan ID set kontrol dari langkah dua.
 - [controlId](#)— Gunakan ID kontrol dari langkah kedua.
 - [manualEvidence](#)— Gunakan `textResponse` sebagai jenis bukti manual dan masukkan teks yang ingin Anda simpan sebagai bukti manual.

Untuk informasi selengkapnya, pilih salah satu tautan dalam prosedur sebelumnya untuk membaca lebih lanjut di Refer AWS Audit Manager ensi API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasa AWS .

Langkah selanjutnya

Setelah Anda mengumpulkan dan meninjau bukti untuk penilaian Anda, Anda dapat membuat laporan penilaian. Untuk informasi selengkapnya, lihat [Menyiapkan laporan penilaian di AWS Audit Manager](#).

Format file yang didukung untuk bukti manual

Tabel berikut mencantumkan dan menjelaskan jenis file yang dapat Anda unggah sebagai bukti manual. Untuk setiap jenis file, tabel juga mencantumkan ekstensi file yang didukung.

Tipe file	Deskripsi	Ekstensi file yang didukung
Kompresi atau arsip	Arsip terkompresi GNU Zip dan arsip terkompresi ZIP	.gz, .zip
Dokumen	File dokumen umum seperti PDF dan file Microsoft Office	.doc, .docx, .pdf, .ppt, .pptx, .xls, .xlsx
Citra	File gambar dan grafik	.jpeg, .jpg, .png, .svg
Teks	File teks non-biner lainnya, seperti dokumen teks biasa dan file bahasa markup	.cer, .csv, .html, .jmx, .json, .md, .out, .rtf, .txt, .xml, .yaml, .yml

Sumber daya tambahan

Tinjau halaman-halaman berikut untuk mempelajari tentang berbagai cara yang dapat Anda tambahkan bukti Anda sendiri ke kontrol penilaian.

- [Mengimpor file bukti manual dari Amazon S3](#)
- [Mengunggah file bukti manual dari browser Anda](#)
- [Memasukkan tanggapan teks bentuk bebas sebagai bukti manual](#)

Menyiapkan laporan penilaian di AWS Audit Manager

Setelah Anda mengumpulkan dan meninjau bukti untuk penilaian Anda, Anda dapat membuat laporan penilaian. Laporan penilaian merangkum penilaian Anda dan menyediakan tautan ke sekumpulan folder terorganisir yang berisi bukti terkait.

Poin kunci

Newly-collected bukti tidak secara otomatis muncul dalam laporan penilaian. Ini berarti Anda dapat mengontrol bukti mana yang ingin Anda sertakan dalam laporan. Setelah memilih bukti yang ingin Anda sertakan, Anda dapat membuat laporan penilaian akhir untuk dibagikan dengan auditor Anda.

Saat Anda membuat laporan penilaian, laporan tersebut ditempatkan ke dalam bucket S3 yang Anda pilih sebagai tujuan laporan penilaian Anda. Anda juga dapat mengunduh laporan penilaian dari pusat unduhan di Audit Manager.

Sumber daya tambahan

Untuk informasi selengkapnya tentang laporan penilaian dan cara mengelolanya, lihat sumber daya berikut.

- [Menambahkan bukti ke laporan penilaian](#)
- [Menghapus bukti dari laporan penilaian](#)
- [Menghasilkan laporan penilaian](#)
- [Mengunduh laporan penilaian](#)
- [Menavigasi laporan penilaian dan menjelajahi isinya](#)
- [Memvalidasi laporan penilaian](#)
- [Menghapus laporan penilaian](#)
- [Menghasilkan laporan penilaian dari hasil pencarian pencari bukti](#)
- [Mengkonfigurasi tujuan laporan penilaian default](#)
- [Memecahkan masalah laporan penilaian](#)

Menambahkan bukti ke laporan penilaian

Sebelum Anda dapat membuat laporan penilaian, Anda harus menambahkan setidaknya satu bukti ke laporan penilaian Anda. Anda dapat menambahkan seluruh folder bukti, atau Anda dapat menambahkan item bukti tertentu dari dalam folder.

Prosedur

Untuk memasukkan bukti dalam laporan penilaian, ikuti langkah-langkah ini.

Untuk menambahkan bukti ke laporan penilaian

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi, pilih Penilaian, lalu pilih penilaian.
3. Pada tab Kontrol, gulir ke bawah ke tabel Kumpulan kontrol dan pilih kontrol dengan bukti yang ingin Anda sertakan dalam laporan penilaian.
4. Pilih bagaimana Anda ingin menambahkan bukti ke laporan penilaian Anda.
 - a. Untuk menambahkan seluruh folder bukti, gulir ke bawah ke folder Bukti, pilih folder yang ingin Anda tambahkan, lalu pilih Tambahkan ke laporan penilaian.

Tip

Jika Anda tidak dapat melihat folder yang Anda cari, ubah filter dropdown ke Sepanjang waktu. Jika tidak, Anda akan melihat folder tujuh hari terakhir secara default. Jika Tambahkan ke laporan penilaian berwarna abu-abu, folder bukti sudah ditambahkan ke laporan penilaian.

- b. Untuk menambahkan bukti spesifik, pilih folder bukti untuk membuka isinya. Pilih satu atau beberapa item dari daftar, lalu pilih Tambahkan ke laporan penilaian.

Tip

Jika Tambahkan ke laporan penilaian berwarna abu-abu, pastikan Anda telah mencentang kotak di sebelah bukti, lalu coba lagi.

5. Setelah Anda menambahkan bukti ke laporan penilaian, spanduk sukses hijau muncul. Pilih Lihat bukti dalam laporan penilaian untuk melihat bukti yang akan disertakan dalam laporan penilaian Anda.
 - Atau, Anda dapat melihat bukti yang akan disertakan dalam laporan penilaian Anda dengan menavigasi kembali ke penilaian Anda dan memilih tab pemilihan laporan penilaian.

Langkah selanjutnya

Jika Anda perlu menghapus bukti dari laporan penilaian, lihat [Menghapus bukti dari laporan penilaian](#).

Saat Anda siap untuk membuat laporan penilaian, lihat [Menghasilkan laporan penilaian](#).

Sumber daya tambahan

Untuk menemukan jawaban atas pertanyaan dan masalah umum, lihat [Memecahkan masalah laporan penilaian](#) di bagian Pemecahan Masalah pada panduan ini.

Menghapus bukti dari laporan penilaian

Jika Anda perlu menghapus bukti dari laporan penilaian, ikuti langkah-langkah ini. Anda dapat menghapus seluruh folder bukti, atau Anda dapat menghapus item bukti tertentu dari dalam folder.

Prosedur

Untuk menghapus bukti dari laporan penilaian

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi, pilih Penilaian, lalu pilih nama penilaian untuk membukanya.
3. Pada tab Kontrol, gulir ke bawah ke tabel Kumpulan kontrol dan pilih nama kontrol untuk membukanya.
4. Pilih bagaimana Anda ingin menghapus bukti dari laporan penilaian Anda.
 - a. Untuk menghapus seluruh folder bukti, gulir ke bawah ke folder Bukti, pilih folder yang ingin Anda hapus, lalu pilih Hapus dari laporan penilaian.

Tip

Jika Anda tidak dapat melihat folder yang Anda cari, ubah filter dropdown ke Sepanjang waktu. Jika tidak, Anda akan melihat folder tujuh hari terakhir secara default. Jika Hapus dari laporan penilaian berwarna abu-abu, folder bukti sudah dihapus dari laporan penilaian.

- b. Untuk menghapus bukti tertentu, pilih folder bukti untuk membuka isinya. Pilih satu atau beberapa item dari daftar, lalu pilih Hapus dari laporan penilaian.

 Tip

Jika Hapus dari laporan penilaian berwarna abu-abu, pastikan Anda telah mencentang kotak di sebelah bukti, lalu coba lagi.

5. Setelah Anda menambahkan bukti ke laporan penilaian, spanduk sukses hijau muncul. Pilih Lihat bukti dalam laporan penilaian untuk melihat bukti yang akan disertakan dalam laporan penilaian Anda.
 - Atau, Anda dapat melihat bukti yang akan disertakan dalam laporan penilaian Anda dengan menavigasi kembali ke penilaian Anda dan memilih tab pemilihan laporan penilaian.

Langkah selanjutnya

Saat Anda siap untuk membuat laporan penilaian, lihat [Menghasilkan laporan penilaian](#).

Sumber daya tambahan

Untuk menemukan jawaban atas pertanyaan dan masalah umum, lihat [Memecahkan masalah laporan penilaian](#) di bagian Pemecahan Masalah pada panduan ini.

Menghasilkan laporan penilaian

Saat Anda siap untuk membuat laporan penilaian, ikuti langkah-langkah berikut.

Prasyarat

Sebelum Anda dapat membuat laporan penilaian, Anda harus menambahkan setidaknya satu bukti ke laporan penilaian Anda. Anda dapat menambahkan seluruh folder bukti, atau Anda dapat menambahkan item bukti individual dari dalam folder.

Untuk memastikan bahwa laporan penilaian Anda berhasil dibuat, tinjau laporan kami [Kiat konfigurasi untuk tujuan laporan penilaian Anda](#).

Prosedur

Membuat laporan penilaian

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi kiri, pilih Assessments.

3. Pilih nama penilaian yang ingin Anda buat laporan penilaian.
4. Pilih tab Pemilihan laporan penilaian, lalu pilih Buat laporan penilaian.

 Tip

Jika Generate assessment report berwarna abu-abu, ini berarti belum ada bukti yang ditambahkan ke laporan penilaian.

5. Di jendela pop-up, berikan nama dan deskripsi untuk laporan penilaian, dan tinjau detail laporan penilaian.
6. Pilih Buat laporan penilaian dan tunggu beberapa menit sementara laporan penilaian Anda dibuat.
7. Temukan dan unduh laporan penilaian Anda dari halaman Pusat unduhan di konsol Audit Manager.
 - Atau, Anda dapat pergi ke bucket S3 tujuan laporan penilaian Anda dan mengunduh laporan penilaian dari sana.

Langkah selanjutnya

Setelah membuat laporan penilaian, Anda dapat mempelajari lebih lanjut tentang hal berikut:

- Temukan dan unduh laporan penilaian Anda — Pelajari cara mengunduh laporan penilaian Anda [dari pusat unduhan](#) atau [dari Amazon S3](#).
- Jelajahi laporan penilaian Anda — Pelajari cara [menavigasi laporan penilaian dan jelajahi isinya](#).
- Validasi laporan penilaian Anda — Pelajari cara menggunakan operasi [ValidateAssessmentReportIntegrity](#) API untuk memvalidasi laporan penilaian Anda.
- Hapus laporan penilaian yang tidak diinginkan — Pelajari cara menghapus laporan yang tidak diinginkan [dari pusat unduhan](#) atau [dari Amazon S3](#).
- Hasilkan laporan penilaian dari pencari bukti - Pelajari cara [menghasilkan laporan penilaian dari hasil pencarian pencari bukti Anda](#).

Sumber daya tambahan

Untuk menemukan jawaban atas pertanyaan dan masalah umum, lihat [Memecahkan masalah laporan penilaian](#) di bagian Pemecahan Masalah pada panduan ini.

Mengubah status kontrol penilaian di AWS Audit Manager

Anda dapat mengubah status kontrol penilaian dalam penilaian aktif Anda. Memperbarui status kontrol memungkinkan Anda melacak kemajuannya dan menunjukkan kapan Anda telah meninjaunya, menjaga penilaian Anda tetap teratur dan terbaru.

Prasyarat

Prosedur berikut mengasumsikan bahwa Anda sebelumnya telah membuat penilaian, dan statusnya saat ini aktif.

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk mengelola penilaian di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Anda dapat memperbarui status kontrol penilaian menggunakan konsol Audit Manager, API Manajer Audit, atau AWS Command Line Interface (AWS CLI).

Note

Mengubah status kontrol menjadi Ditinjau adalah final. Setelah menyetel status kontrol ke Ditinjau, Anda tidak dapat lagi mengubah status kontrol tersebut atau kembali ke status sebelumnya.

Audit Manager console

Untuk mengubah status kontrol penilaian di konsol Audit Manager

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi, pilih Assessments.
3. Pilih nama penilaian untuk membukanya.
4. Dari halaman penilaian, pilih tab Kontrol, gulir ke bawah ke tabel Kumpulan kontrol, lalu pilih nama kontrol untuk membukanya.
5. Pilih Perbarui status kontrol di kanan atas halaman, lalu pilih status:

Status	Deskripsi
Dalam peninjauan	Pilih status ini jika Anda belum meninjau kontrol.
Diulas	Pilih status ini jika Anda telah selesai meninjau bukti untuk kontrol ini, dan Anda ingin terus mengumpulkan atau menambahkan bukti.
Tidak aktif	Pilih status ini jika Anda ingin berhenti mengumpulkan bukti otomatis untuk kontrol ini.

6. Pilih Perbarui status kontrol untuk mengonfirmasi pilihan Anda.

AWS CLI

Untuk mengubah status kontrol penilaian di AWS CLI

1. Jalankan perintah [list-assessment](#).

```
aws auditmanager list-assessments
```

Tanggapan mengembalikan daftar penilaian. Temukan penilaian yang berisi kontrol yang ingin Anda perbarui, dan catat ID penilaian.

2. Jalankan [perintah](#) `get-assessment` dan tentukan ID penilaian dari langkah 1.

Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri.

```
aws auditmanager get-assessment --assessment-id 1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4e5f6g
```

Dalam tanggapan, temukan kontrol yang ingin Anda perbarui dan catat ID kontrol dan ID set kontrolnya.

3. Jalankan [perintah](#) `update-assessment` control dan tentukan parameter berikut:
 - `--assessment-id`— Penilaian yang dimiliki kontrol.
 - `--control-set-id`— Kumpulan kontrol yang dimiliki kontrol tersebut.
 - `--control-id`— Kontrol yang ingin Anda perbarui.

- `--control-status`— Tetapkan nilai ini ke `UNDER_REVIEW`, `REVIEWED`, atau `INACTIVE`.

Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri.

```
aws auditmanager update-assessment-control --assessment-id 1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4e5f6g --control-set-id "My control set" --control-id 2b3c4d5e-2b3c-2b3c-2b3c-2b3c4d5f6g7h --control-status REVIEWED
```

Audit Manager API

Untuk mengubah status kontrol penilaian menggunakan API

1. Gunakan [ListAssessments](#) operasi.

Dalam tanggapan, temukan penilaian yang berisi kontrol yang ingin Anda perbarui, dan catat ID penilaian.

2. Gunakan [GetAssessment](#) operasi dan tentukan ID penilaian dari langkah 1.

Dalam tanggapan, temukan kontrol yang ingin Anda perbarui dan catat ID kontrol dan ID set kontrolnya.

3. Gunakan [UpdateAssessmentControl](#) operasi dan tentukan parameter berikut:

- [assessmentId](#)— Penilaian yang dimiliki kontrol.
- [controlSetId](#)— Kumpulan kontrol yang dimiliki kontrol tersebut.
- [controlId](#)— Kontrol yang ingin Anda perbarui.
- [controlStatus](#)— Tetapkan nilai ini ke `UNDER_REVIEW`, `REVIEWED`, atau `INACTIVE`.

Untuk informasi selengkapnya tentang operasi API ini, pilih salah satu tautan di prosedur sebelumnya untuk membaca lebih lanjut di Refer AWS Audit Manager ensi API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasa AWS .

Langkah selanjutnya

Saat Anda siap untuk mengubah status penilaian, lihat [Mengubah status penilaian menjadi tidak aktif di AWS Audit Manager](#).

Mengubah status penilaian menjadi tidak aktif di AWS Audit Manager

Jika Anda tidak perlu lagi mengumpulkan bukti untuk penilaian, Anda dapat mengubah status penilaian menjadi Tidak aktif. Ketika status penilaian berubah menjadi tidak aktif, penilaian berhenti mengumpulkan bukti. Akibatnya, Anda tidak lagi dikenakan biaya apa pun untuk penilaian itu.

Selain menghentikan pengumpulan bukti, Audit Manager membuat perubahan berikut pada kontrol yang berada dalam penilaian tidak aktif:

- Semua set kontrol berubah menjadi status Tinjau.
- Semua kontrol yang sedang ditinjau berubah menjadi status Tinjau.
- Delegasi untuk penilaian tidak aktif tidak dapat lagi melihat atau mengedit kontrol dan kumpulan kontrolnya.

Prasyarat

Prosedur berikut mengasumsikan bahwa Anda sebelumnya telah membuat penilaian, dan statusnya saat ini aktif.

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk mengelola penilaian di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Anda dapat memperbarui status penilaian menggunakan konsol Audit Manager, API Manajer Audit, atau AWS Command Line Interface (AWS CLI).

Warning

Tindakan ini tidak dapat diubah. Kami menyarankan Anda melanjutkan dengan hati-hati dan memastikan bahwa Anda ingin menandai penilaian Anda sebagai tidak aktif. Ketika penilaian tidak aktif, Anda memiliki akses baca-saja ke isinya. Ini berarti bahwa Anda masih dapat meninjau bukti yang dikumpulkan sebelumnya dan menghasilkan laporan penilaian.

Namun, Anda tidak dapat mengedit penilaian yang tidak aktif, menambahkan komentar, atau mengunggah bukti manual apa pun.

Audit Manager console

Untuk mengubah status penilaian menjadi tidak aktif di konsol Audit Manager

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi, pilih Assess ments.
3. Pilih nama penilaian untuk membukanya.
4. Di sudut kanan atas halaman, pilih Per barui status penilaian, lalu pilih Tidak aktif.
5. Pilih Perbarui status di jendela pop-up untuk mengonfirmasi bahwa Anda ingin mengubah status menjadi tidak aktif.

Perubahan penilaian dan kontrolnya mulai berlaku setelah sekitar satu menit.

AWS CLI

Untuk mengubah status penilaian menjadi tidak aktif di AWS CLI

1. Pertama, identifikasi penilaian yang ingin Anda perbarui. Untuk melakukan ini, jalankan perintah [list-assessment](#).

```
aws auditmanager list-assessments
```

Tanggapan mengembalikan daftar penilaian. Temukan penilaian yang ingin Anda nonaktifkan, dan catat ID penilaian.

2. Selanjutnya, jalankan [perintah](#) update-assessment status dan tentukan parameter berikut:
 - `--assessment-id`—Gunakan parameter ini untuk menentukan penilaian yang ingin Anda nonaktifkan.
 - `--status` – Atur nilai ini ke INACTIVE.

Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri.

```
aws auditmanager update-assessment-status --assessment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --status INACTIVE
```

Perubahan penilaian dan kontrolnya mulai berlaku setelah sekitar satu menit.

Audit Manager API

Untuk mengubah status penilaian menjadi tidak aktif menggunakan API

1. Gunakan [ListAssessments](#) operasi untuk menemukan penilaian yang ingin Anda nonaktifkan, dan catat ID penilaian.
2. Gunakan [UpdateAssessmentStatus](#) operasi dan tentukan parameter berikut:
 - [AssessmentID](#) — Gunakan parameter ini untuk menentukan penilaian yang ingin Anda nonaktifkan.
 - [status](#) — Tetapkan nilai ini keINACTIVE.

Perubahan penilaian dan kontrolnya mulai berlaku setelah sekitar satu menit.

Untuk informasi selengkapnya tentang operasi API ini, pilih salah satu tautan di prosedur sebelumnya untuk membaca lebih lanjut di Refer AWS Audit Manager ensi API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasa AWS .

Langkah selanjutnya

Jika Anda yakin bahwa Anda tidak lagi memerlukan penilaian yang tidak aktif, Anda dapat membersihkan lingkungan Manajer Audit dengan menghapus penilaian. Untuk petunjuk, lihat [Menghapus penilaian di AWS Audit Manager](#).

Menghapus penilaian di AWS Audit Manager

Ketika Anda tidak lagi memerlukan penilaian, Anda dapat menghapusnya dari lingkungan Manajer Audit Anda. Ini memungkinkan Anda untuk membersihkan ruang kerja Anda dan fokus pada penilaian yang relevan dengan tugas dan prioritas Anda saat ini.

 Tip

Jika tujuan Anda adalah mengurangi biaya, pertimbangkan untuk [mengubah status penilaian menjadi tidak aktif](#) alih-alih menghapusnya. Tindakan ini menghentikan pengumpulan bukti, dan menempatkan penilaian Anda dalam keadaan baca-saja di mana Anda dapat meninjau bukti yang sebelumnya dikumpulkan. Penilaian yang tidak aktif tidak dikenakan biaya apa pun.

Prasyarat

Prosedur berikut mengasumsikan bahwa Anda sebelumnya telah membuat penilaian.

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk menghapus penilaian di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Anda dapat menghapus penilaian menggunakan konsol Audit Manager, API Manajer Audit atau AWS Command Line Interface (AWS CLI).

 Warning

Tindakan ini secara permanen menghapus penilaian Anda dan semua bukti yang dikumpulkan. Anda tidak dapat memulihkan data ini. Oleh karena itu, kami sarankan Anda melanjutkan dengan hati-hati dan memastikan bahwa Anda ingin menghapus penilaian Anda.

Audit Manager console

Untuk menghapus penilaian di konsol Audit Manager

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi, pilih Assess ments.
3. Pilih penilaian yang ingin Anda hapus, lalu pilih H apus.

AWS CLI

Untuk menghapus penilaian di AWS CLI

1. Pertama, identifikasi penilaian yang ingin Anda hapus. Untuk melakukan ini, jalankan perintah [list-assessment](#).

```
aws auditmanager list-assessments
```

Tanggapan mengembalikan daftar penilaian. Temukan penilaian yang ingin Anda hapus, dan catat ID penilaian.

2. Selanjutnya, gunakan [perintah](#) delete-assessment dan tentukan --assessment-id penilaian yang ingin Anda hapus.

Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri.

```
aws auditmanager delete-assessment --assessment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

Untuk menghapus penilaian menggunakan API

1. Gunakan [ListAssessments](#) operasi untuk menemukan penilaian yang ingin Anda hapus.

Dalam tanggapan, perhatikan ID penilaian.

2. Gunakan [DeleteAssessment](#) operasi dan tentukan [AssessmentID](#) penilaian yang ingin Anda hapus.

Untuk informasi selengkapnya tentang operasi API ini, pilih salah satu tautan sebelumnya untuk membaca lebih lanjut di Refer AWS Audit Manager ensi API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasa AWS .

Sumber daya tambahan

Untuk informasi tentang retensi data di Audit Manager, lihat [Penghapusan data Audit Manager](#).

Delegasi di AWS Audit Manager

Saat Anda menavigasi proses penilaian di AWS Audit Manager, Anda mungkin menghadapi situasi di mana Anda memerlukan bantuan dari pakar materi pelajaran untuk meninjau dan memvalidasi bukti yang dikumpulkan. Di sinilah konsep delegasi ikut bermain.

Poin kunci

Delegasi memungkinkan [pemilik audit](#) untuk menetapkan set kontrol khusus kepada [delegasi](#) — individu dengan keahlian khusus di bidang yang relevan. Dengan menggunakan fitur delegasi, Anda dapat memastikan bahwa bukti untuk setiap kontrol dievaluasi secara menyeluruh oleh personel yang sesuai. Ini membantu Anda merampingkan proses peninjauan dan meningkatkan akurasi dan keandalan penilaian Anda secara keseluruhan. Apakah Anda memerlukan panduan untuk menafsirkan bukti teknis, mengklarifikasi persyaratan kepatuhan, atau mendapatkan wawasan yang lebih dalam tentang domain tertentu, delegasi memungkinkan Anda untuk berkolaborasi secara efektif dengan pakar materi pelajaran.

Pada tingkat tinggi, proses delegasi adalah sebagai berikut:

1. Pemilik audit memilih kontrol yang ditetapkan dalam penilaian mereka dan mendelegasikannya untuk ditinjau.
2. Delegasi meninjau kontrol dan bukti mereka, dan menyerahkan kontrol yang ditetapkan kembali ke pemilik audit setelah selesai.
3. Pemilik audit diberi tahu bahwa peninjauan selesai, dan memeriksa kontrol yang ditinjau untuk setiap komentar dari delegasi.

Note

An Akun AWS dapat menjadi pemilik audit atau delegasi yang berbeda Wilayah AWS.

Sumber daya tambahan

Gunakan bagian berikut dari Bab ini untuk mempelajari lebih lanjut tentang cara mengelola tugas delegasi di AWS Audit Manager.

- [Memahami tugas delegasi yang berbeda untuk pemilik audit](#)
 - [Mendelegasikan set kontrol untuk ditinjau AWS Audit Manager](#)
 - [Menemukan dan meninjau delegasi yang telah Anda kirim AWS Audit Manager](#)
 - [Menghapus delegasi Anda yang sudah selesai di AWS Audit Manager](#)
- [Memahami tugas delegasi yang berbeda untuk delegasi](#)
 - [Melihat notifikasi untuk permintaan delegasi yang masuk](#)
 - [Meninjau set kontrol yang didelegasikan dan bukti terkait](#)
 - [Menambahkan komentar tentang kontrol selama tinjauan set kontrol](#)
 - [Menandai kontrol seperti yang ditinjau dalam AWS Audit Manager](#)
 - [Mengirimkan kontrol yang ditinjau kembali ke pemilik audit](#)

Memahami tugas delegasi yang berbeda untuk pemilik audit

Sebagai pemilik audit di AWS Audit Manager, Anda bertanggung jawab untuk mengelola penilaian dan memastikan kepatuhan dalam organisasi Anda. Meskipun Anda memiliki keahlian dalam tata kelola, risiko, dan kepatuhan, mungkin ada saat-saat ketika Anda memiliki pertanyaan atau memerlukan bantuan dari pakar materi pelajaran untuk meninjau dan menafsirkan bukti atau kontrol teknis tertentu. Di sinilah fitur delegasi di Audit Manager menjadi berguna.

Poin kunci

Membuat delegasi memungkinkan Anda menetapkan set kontrol dalam penilaian kepada pengguna Audit Manager lainnya (dikenal sebagai [delegasi](#)) yang memiliki pengetahuan khusus atau keahlian teknis di bidang yang relevan. Delegasi ini kemudian dapat meninjau set kontrol yang ditugaskan, menganalisis bukti yang dikumpulkan, memberikan komentar atau bukti tambahan jika diperlukan, dan memperbarui status kontrol individu.

Proses delegasi merampingkan peninjauan dan validasi kontrol dengan memanfaatkan keahlian kolektif dalam organisasi Anda. Ini memastikan bahwa setiap kontrol dievaluasi secara menyeluruh oleh personel yang paling berkualitas, meningkatkan akurasi dan keandalan penilaian Anda.

Sumber daya tambahan

Bagian berikut memandu Anda melalui berbagai tugas yang terkait dengan mengelola delegasi sebagai pemilik audit. Ini termasuk cara mendelegasikan set kontrol, melacak status delegasi,

dan mengelola delegasi yang telah selesai. Dengan menggunakan delegasi secara efektif, Anda dapat berkolaborasi dengan pakar materi pelajaran, memanfaatkan pengetahuan khusus mereka, dan mempertahankan proses audit yang komprehensif dan terinformasi dengan baik dalam Audit Manager.

- [Mendelegasikan set kontrol untuk ditinjau AWS Audit Manager](#)
- [Menemukan dan meninjau delegasi yang telah Anda kirim AWS Audit Manager](#)
- [Menghapus delegasi Anda yang sudah selesai di AWS Audit Manager](#)

Mendelegasikan set kontrol untuk ditinjau AWS Audit Manager

Ketika Anda membutuhkan bantuan dari ahli materi pelajaran, Anda dapat memilih Akun AWS yang ingin Anda bantu, dan kemudian mendelegasikan set kontrol kepada mereka untuk ditinjau.

Mendelegasikan izin

Kebijakan di bawah ini dilampirkan ke delegasi kepada siapa set kontrol didelegasikan.

Audit Manager mengganti *placeholder text* dengan akun dan pengenalan sumber daya Anda sebelum melampirkan kebijakan.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Delegate",
      "Effect": "Allow",
      "Principal": {
        "AWS": "Principal for user/role who is delegated a Control Set of the Assessment"
      },
      "Action": [
        "auditmanager:UpdateAssessmentControl",
        "auditmanager:UpdateAssessmentControlSetStatus",
        "auditmanager:GetEvidenceFoldersByAssessmentControl",
        "auditmanager:BatchImportEvidenceToAssessmentControl",
        "auditmanager:GetEvidenceFolder",

```



```
        "auditmanager:GetEvidence",
        "auditmanager:GetEvidenceByEvidenceFolder"
    ],
    "Resource": "arn:aws:auditmanager:us-  
east-1:123456789012:assessment/assessment_ID/controlSet/control_set_ID"
  }
]
}
```

Prasyarat

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk membuat delegasi. AWS Audit Manager Dua kebijakan yang disarankan yang memberikan izin ini adalah [Izinkan pengguna akses administrator penuh ke AWS Audit Manager](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Anda dapat menggunakan salah satu dari prosedur berikut untuk mendelegasikan set kontrol.

Mendelegasikan set kontrol dari halaman penilaian

Untuk mendelegasikan set kontrol dari halaman penilaian

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.
2. Di panel navigasi, pilih Penilaian.
3. Pilih nama penilaian yang berisi set kontrol yang ingin Anda delegasikan.
4. Dari halaman penilaian, pilih tab Kontrol. Ini menampilkan ringkasan status kontrol dan daftar kontrol dalam penilaian.
5. Pilih set kontrol dan pilih Set kontrol delegasi.
6. Di bawah pilihan Delegasi, daftar pengguna dan peran ditampilkan. Pilih pengguna atau peran, atau gunakan bilah pencarian untuk mencarinya.
7. Di bawah Detail delegasi, tinjau nama set kontrol dan nama penilaian.
8. (Opsional) Di bawah Komentar, tambahkan komentar dengan instruksi untuk membantu delegasi memenuhi tugas peninjauan mereka. Jangan sertakan informasi sensitif apa pun dalam komentar Anda.
9. Pilih set kontrol delegasi.

10. Spanduk sukses hijau menegaskan delegasi yang berhasil dari set kontrol. Pilih Lihat delegasi untuk melihat permintaan delegasi. Anda juga dapat melihat delegasi kapan saja dengan memilih Delegasi di panel navigasi kiri konsol. AWS Audit Manager

Mendelegasikan set kontrol dari halaman delegasi

Untuk mendelegasikan set kontrol dari halaman delegasi

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.
2. Di panel navigasi, pilih Delegasi.
3. Dari halaman delegasi, pilih Buat delegasi.
4. Di bawah Pilih set penilaian dan kontrol, tentukan penilaian dan set kontrol yang ingin Anda delegasikan.
5. Di bawah pilihan Delegasi, Anda akan melihat daftar pengguna dan peran. Pilih pengguna atau peran, atau gunakan bilah pencarian untuk mencarinya.
6. (Opsional) Di bawah Komentar, tambahkan komentar dengan instruksi untuk membantu delegasi memenuhi tugas peninjauan mereka. Jangan sertakan informasi sensitif apa pun dalam komentar Anda.
7. Pilih Buat delegasi.
8. Spanduk sukses hijau menegaskan delegasi yang berhasil dari set kontrol. Pilih Lihat delegasi untuk melihat permintaan delegasi. Anda juga dapat melihat delegasi kapan saja dengan memilih Delegasi di panel navigasi kiri konsol. AWS Audit Manager

Setelah Anda mendelegasikan set kontrol untuk ditinjau, delegasi menerima pemberitahuan dan kemudian dapat mulai meninjau set kontrol. Proses yang diikuti delegasi ini dijelaskan dalam [Memahami tugas delegasi yang berbeda untuk delegasi](#).

Langkah selanjutnya

Untuk meninjau kembali delegasi Anda di kemudian hari, lihat. [Menemukan dan meninjau delegasi yang telah Anda kirim AWS Audit Manager](#)

Menemukan dan meninjau delegasi yang telah Anda kirim AWS Audit Manager

Anda dapat mengakses daftar delegasi kapan saja dengan memilih Delegasi di panel navigasi kiri Audit Manager. Halaman delegasi berisi daftar delegasi aktif dan selesai Anda.

Ketika delegasi selesai, Anda menerima pemberitahuan di Audit Manager. Anda mungkin juga menerima komentar dengan komentar dari delegasi. Prosedur berikut menjelaskan cara memeriksa delegasi Anda di Audit Manager setelah selesai, dan cara melihat komentar apa pun yang mungkin ditinggalkan delegasi untuk Anda.

Prasyarat

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk melihat delegasi. AWS Audit Manager Dua kebijakan yang disarankan yang memberikan izin ini adalah [Izinkan pengguna akses administrator penuh ke AWS Audit Manager](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Ikuti langkah-langkah ini untuk menemukan dan meninjau delegasi yang sebelumnya Anda buat.

Untuk melihat delegasi yang telah selesai dan memeriksa komentar

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.
2. Di panel navigasi, pilih Delegasi.
3. Tinjau halaman Delegasi, yang mencakup tabel dengan informasi berikut:

Nama	Deskripsi
Delegasikan ke	Akun AWS Yang Anda delegasikan kontrol diatur ke.
Tanggal	Tanggal ketika Anda mendelegasikan set kontrol.
Status	Status delegasi saat ini.
Penilaian	Nama penilaian dengan tautan ke halaman detail penilaian.
Set kontrol	Nama set kontrol yang didelegasikan untuk ditinjau.

4. Temukan set penilaian dan kontrol yang ditinjau dan diserahkan oleh delegasi kepada Anda, dan pilih nama penilaian untuk membukanya.
5. Di bawah tab Kontrol pada halaman detail penilaian, gulir ke bawah ke tabel Set kontrol.

6. Di bawah Kontrol yang dikelompokkan berdasarkan set kontrol, temukan nama set kontrol yang Anda delegasikan.
7. Perluas nama set kontrol untuk menampilkan kontrolnya, dan pilih nama kontrol untuk membuka halaman detail kontrol.
8. Pilih tab Komentar untuk melihat komentar apa pun yang ditambahkan oleh delegasi untuk kontrol tertentu.
9. Jika Anda puas bahwa peninjauan selesai untuk set kontrol, pilih set kontrol dan pilih Tinjauan set kontrol lengkap.

Important

Audit Manager mengumpulkan bukti secara terus menerus. Akibatnya, bukti baru tambahan dapat dikumpulkan setelah delegasi menyelesaikan peninjauan kontrol mereka.

Jika Anda hanya ingin menggunakan bukti yang ditinjau dalam laporan penilaian Anda, Anda dapat merujuk ke stempel waktu kontrol yang ditinjau untuk menentukan kapan bukti ditinjau. Stempel waktu ini dapat ditemukan di [Tab Changelog](#) halaman detail kontrol. Anda kemudian dapat menggunakan stempel waktu ini untuk mengidentifikasi bukti mana yang Anda tambahkan ke laporan penilaian Anda.

Langkah selanjutnya

Untuk menghapus delegasi setelah selesai dan Anda tidak lagi membutuhkannya, lihat [Menghapus delegasi Anda yang sudah selesai di AWS Audit Manager](#).

Menghapus delegasi Anda yang sudah selesai di AWS Audit Manager

Mungkin ada keadaan di mana Anda membuat delegasi tetapi nantinya tidak lagi memerlukan bantuan untuk meninjau set kontrol tersebut. Jika ini terjadi, Anda dapat menghapus delegasi aktif di Audit Manager. Anda juga dapat menghapus delegasi yang sudah selesai yang tidak ingin Anda lihat lagi di halaman delegasi.

Prasyarat

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk menghapus delegasi. AWS Audit Manager Dua kebijakan yang disarankan yang memberikan izin ini adalah [Izinkan pengguna akses](#)

[administrator penuh ke AWS Audit Manager](#) dan [izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Untuk menghapus delegasi

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.
2. Di panel navigasi, pilih Delegasi.
3. Pada halaman Delegasi, pilih delegasi yang ingin Anda batalkan, lalu pilih Hapus delegasi.
4. Di jendela pop-up yang muncul, pilih Hapus untuk mengonfirmasi pilihan Anda.

Memahami tugas delegasi yang berbeda untuk delegasi

Sebagai delegasi AWS Audit Manager, Anda memainkan peran penting dalam mendukung pemilik audit selama proses penilaian. Meskipun [pemilik audit](#) bertanggung jawab untuk mengelola penilaian dan memastikan kepatuhan secara keseluruhan, mereka terkadang memerlukan bantuan dari pakar materi pelajaran dengan meninjau dan menafsirkan bukti teknis spesifik yang berada di luar bidang keahlian mereka. Dalam skenario seperti itu, pengetahuan dan keterampilan Anda menjadi sangat berharga.

Poin kunci

Fitur delegasi memungkinkan pemilik audit untuk menetapkan set kontrol khusus kepada Anda untuk ditinjau, memanfaatkan keahlian bisnis atau teknis khusus Anda. Pendekatan kolaboratif ini tidak hanya meningkatkan akurasi dan keandalan penilaian tetapi juga merampingkan proses peninjauan, memungkinkan pemilik audit untuk fokus pada tanggung jawab inti mereka sementara Anda memusatkan upaya Anda pada bidang di mana keahlian Anda paling berharga.

Sebagai delegasi, Anda mungkin menerima permintaan dari pemilik audit untuk meninjau bukti yang terkait dengan set kontrol yang ditetapkan. Anda dapat membantu pemilik audit dengan meninjau set kontrol dan bukti terkait mereka, menambahkan komentar, mengunggah bukti tambahan, dan memperbarui status setiap kontrol yang Anda tinjau.

Note

Pemilik audit mendelegasikan set kontrol khusus untuk ditinjau, bukan seluruh penilaian. Akibatnya, delegasi memiliki akses terbatas ke penilaian. Delegasi dapat meninjau bukti,

menambahkan komentar, mengunggah bukti manual, dan memperbarui status kontrol untuk setiap kontrol dalam set kontrol. Untuk informasi selengkapnya tentang peran dan izin di Audit Manager, lihat [Kebijakan yang disarankan untuk persona pengguna di AWS Audit Manager](#).

Sumber daya tambahan

Di bagian berikut, Anda dapat mempelajari lebih lanjut tentang tugas yang terkait dengan mengelola delegasi sebagai delegasi. Ini termasuk cara melihat permintaan delegasi yang masuk, meninjau set kontrol yang ditetapkan, memberikan komentar dan bukti tambahan, dan mengirimkan kontrol Anda yang ditinjau kembali ke pemilik audit.

- [Melihat notifikasi untuk permintaan delegasi yang masuk](#)
- [Meninjau set kontrol yang didelegasikan dan bukti terkait](#)
- [Menambahkan komentar tentang kontrol selama tinjauan set kontrol](#)
- [Menandai kontrol seperti yang ditinjau dalam AWS Audit Manager](#)
- [Mengirimkan kontrol yang ditinjau kembali ke pemilik audit](#)

Melihat notifikasi untuk permintaan delegasi yang masuk

Ketika pemilik audit meminta bantuan Anda untuk meninjau set kontrol, Anda menerima pemberitahuan yang memberi tahu Anda tentang set kontrol yang mereka delegasikan kepada Anda.

Prasyarat

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk melihat notifikasi. AWS Audit Manager Dua kebijakan yang disarankan yang memberikan izin ini adalah [Izinkan pengguna akses administrator penuh ke AWS Audit Manager](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Untuk melihat notifikasi

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.
2. Pilih Notifikasi di panel navigasi kiri.

3. Pada halaman Notifikasi, tinjau daftar set kontrol yang telah didelegasikan kepada Anda untuk ditinjau. Tabel tersebut mencakup informasi berikut:

Nama	Deskripsi
Tanggal	Tanggal ketika set kontrol didelegasikan.
Penilaian	Nama penilaian yang terkait dengan set kontrol.
Set kontrol	Nama set kontrol.
Sumber	Pengguna atau peran yang mendelegasikan set kontrol kepada Anda.
Deskripsi	Instruksi yang disediakan oleh pemilik audit.

 Tip

Anda juga dapat berlangganan topik SNS untuk menerima peringatan email saat set kontrol didelegasikan kepada Anda untuk ditinjau. Untuk informasi selengkapnya, lihat [Pemberitahuan di AWS Audit Manager](#).

Langkah selanjutnya

Saat Anda siap untuk mulai meninjau kontrol yang didelegasikan kepada Anda, lihat. [Meninjau set kontrol yang didelegasikan dan bukti terkait](#)

Meninjau set kontrol yang didelegasikan dan bukti terkait

Anda dapat membantu pemilik audit dengan meninjau set kontrol yang telah mereka delegasikan kepada Anda.

Anda dapat memeriksa kontrol ini dan bukti terkait untuk menentukan apakah ada tindakan tambahan yang diperlukan. Tindakan tambahan tersebut dapat mencakup [mengunggah bukti tambahan secara manual](#) untuk menunjukkan kepatuhan, atau [meninggalkan komentar yang](#) merinci langkah-langkah perbaikan yang Anda ikuti.

Prasyarat

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk melihat set kontrol. AWS Audit Manager Dua kebijakan yang disarankan yang memberikan izin ini adalah [Izinkan pengguna akses administrator penuh ke AWS Audit Manager](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Untuk meninjau set kontrol

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.
2. Di panel navigasi, pilih Pemberitahuan.
3. Pada halaman Notifikasi, Anda dapat melihat daftar set kontrol yang didelegasikan kepada Anda. Identifikasi set kontrol mana yang ingin Anda tinjau, dan pilih nama penilaian terkait untuk membuka halaman detail penilaian.
4. Di bawah tab Kontrol pada halaman detail penilaian, gulir ke bawah ke tabel Set kontrol.
5. Di bawah kolom Kontrol yang dikelompokkan berdasarkan set kontrol, perluas nama set kontrol untuk menampilkan kontrolnya.
6. Pilih nama kontrol untuk membuka halaman detail kontrol.
7. (Opsional) Pilih Perbarui status kontrol untuk mengubah status kontrol. Saat peninjauan sedang berlangsung, Anda dapat menandai status sebagai Dalam Tinjauan.
8. Tinjau informasi tentang kontrol di folder Bukti, Detail, Sumber data, Komentar, dan tab Changelog.
 - Untuk mempelajari tentang masing-masing tab ini dan cara memahami data yang dikandungnya, lihat [Meninjau kontrol penilaian di AWS Audit Manager](#).

Untuk meninjau bukti untuk kontrol

1. Dari halaman detail kontrol, pilih tab Folder bukti.
2. Arahkan ke tabel Folder bukti untuk melihat daftar folder yang berisi bukti untuk kontrol tersebut. Folder ini diatur dan diberi nama berdasarkan tanggal ketika bukti dikumpulkan.
3. Pilih nama folder bukti untuk membukanya. Kemudian, tinjau ringkasan semua bukti yang dikumpulkan pada tanggal tersebut.

- Ringkasan ini mencakup jumlah total masalah pemeriksaan kepatuhan yang dilaporkan langsung dari AWS Security Hub CSPM, AWS Config, atau keduanya.
 - Untuk mempelajari lebih lanjut tentang informasi ini, lihat [Meninjau folder bukti di AWS Audit Manager](#).
4. Dari halaman ringkasan folder bukti, buka tabel Bukti. Di bawah kolom Waktu, pilih bukti untuk dibuka.
 5. Tinjau detail bukti.
 - Untuk mempelajari lebih lanjut tentang informasi ini, lihat [Meninjau bukti di AWS Audit Manager](#).

Langkah selanjutnya

Dalam beberapa kasus, Anda mungkin perlu memberikan bukti tambahan untuk menunjukkan kepatuhan. Dalam kasus ini, Anda dapat mengunggah bukti secara manual. Untuk petunjuk, lihat [Menambahkan bukti manual di AWS Audit Manager](#).

Jika Anda ingin meninggalkan komentar tentang satu atau lebih kontrol yang didelegasikan kepada Anda, lihat [Menambahkan komentar tentang kontrol selama tinjauan set kontrol](#).

Menambahkan komentar tentang kontrol selama tinjauan set kontrol

Anda dapat menambahkan komentar untuk kontrol apa pun yang Anda tinjau. Komentar ini dapat dilihat oleh pemilik audit.

Prasyarat

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk menambahkan komentar ke kontrol penilaian. AWS Audit Manager Dua kebijakan yang disarankan yang memberikan izin ini adalah [Izinkan pengguna akses administrator penuh ke AWS Audit Manager](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Untuk menambahkan komentar ke kontrol

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.
2. Pilih Notifikasi di panel navigasi kiri.

3. Pada halaman Notifikasi, tinjau daftar set kontrol yang didelegasikan kepada Anda.
4. Temukan set kontrol yang berisi kontrol yang ingin Anda berikan komentar, lalu pilih nama penilaian terkait untuk membuka penilaian.
5. Pilih tab Controls, gulir ke bawah ke tabel Control sets, lalu pilih nama kontrol untuk membukanya.
6. Pilih tab Komentar.
7. Di bawah Kirim komentar, masukkan komentar Anda di kotak teks.
8. Pilih Kirim komentar untuk menambahkan komentar Anda. Komentar Anda kemudian muncul di bawah bagian Komentar sebelumnya di halaman, bersama dengan komentar lain mengenai kontrol ini.

Langkah selanjutnya

Setelah selesai meninjau kontrol, ikuti langkah-langkahnya. [Menandai kontrol seperti yang ditinjau dalam AWS Audit Manager](#)

Menandai kontrol seperti yang ditinjau dalam AWS Audit Manager

Anda dapat menunjukkan kemajuan peninjauan Anda dengan memperbarui status kontrol individual dalam set kontrol.

Mengubah status kontrol adalah opsional. Namun, kami menyarankan agar Anda mengubah status setiap kontrol menjadi Ditinjau saat Anda menyelesaikan peninjauan untuk kontrol tersebut. Terlepas dari status masing-masing kontrol individu, Anda masih dapat mengirimkan kontrol kembali ke pemilik audit.

Prasyarat

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk memperbarui status kontrol penilaian. AWS Audit Manager Dua kebijakan yang disarankan yang memberikan izin ini adalah [Izinkan pengguna akses administrator penuh ke AWS Audit Manager](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Untuk menandai kontrol sebagai ditinjau

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.

2. Pilih Notifikasi di panel navigasi kiri.
3. Pada halaman Notifikasi, tinjau daftar set kontrol yang didelegasikan kepada Anda.
4. Temukan set kontrol yang ingin Anda tandai sebagai ditinjau, lalu pilih nama penilaian terkait untuk membuka penilaian.
5. Di bawah tab Kontrol pada halaman detail penilaian, gulir ke bawah ke tabel Set kontrol.
6. Di bawah kolom Kontrol yang dikelompokkan berdasarkan set kontrol, perluas nama set kontrol untuk menampilkan kontrolnya.
7. Pilih nama kontrol untuk membuka halaman detail kontrol.
8. Pilih Perbarui status kontrol dan ubah status menjadi Ditinjau.
9. Di jendela pop-up yang muncul, pilih Perbarui status kontrol untuk mengonfirmasi bahwa Anda selesai meninjau kontrol.

Langkah selanjutnya

Untuk menyelesaikan proses delegasi, lihat [Mengirimkan kontrol yang ditinjau kembali ke pemilik audit](#).

Mengirimkan kontrol yang ditinjau kembali ke pemilik audit

Setelah meninjau set kontrol, menambahkan komentar atau bukti tambahan, dan memperbarui status kontrol individu, Anda mencapai langkah penting — mengirimkan kontrol yang ditinjau kembali ke pemilik audit. Mengirimkan set kontrol yang ditinjau menandai penyelesaian tugas yang didelegasikan, dan memungkinkan pemilik audit untuk memasukkan wawasan dan rekomendasi Anda ke dalam penilaian keseluruhan.

Prasyarat

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk mengirimkan kontrol yang ditinjau kembali ke pemilik audit di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [Izinkan pengguna akses administrator penuh ke AWS Audit Manager](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Ikuti langkah-langkah ini untuk mengirimkan set kontrol ke pemilik audit.

Untuk mengirimkan kontrol yang ditinjau kembali ke pemilik audit

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.
2. Pilih Notifikasi di panel navigasi kiri.
3. Tinjau daftar set kontrol yang didelegasikan kepada Anda. Temukan set kontrol yang ingin Anda kirimkan kembali ke pemilik audit, dan pilih nama penilaian terkait.
4. Gulir ke bawah ke tabel Set kontrol, pilih set kontrol yang ingin Anda kirimkan ke pemilik audit, lalu pilih Kirim untuk ditinjau.
5. Di jendela pop-up yang muncul, Anda dapat menambahkan komentar sebelum memilih Kirim untuk ditinjau.

Laporan penilaian

Laporan penilaian merangkum bukti terpilih yang dikumpulkan untuk penilaian. Ini juga berisi tautan ke file PDF dengan detail tentang setiap bukti. Konten spesifik, organisasi, dan konvensi penamaan laporan penilaian bergantung pada parameter yang Anda pilih saat [membuat laporan](#).

Laporan penilaian membantu Anda memilih dan menyusun bukti yang relevan untuk audit Anda. Namun, mereka tidak menilai kepatuhan bukti itu sendiri. Sebagai gantinya, Audit Manager hanya memberikan rincian bukti yang dipilih sebagai output yang dapat Anda bagikan dengan auditor Anda.

Daftar Isi

- [Memahami struktur folder laporan penilaian](#)
- [Menavigasi laporan penilaian](#)
- [Meninjau bagian dari laporan penilaian](#)
 - [Halaman sampul](#)
 - [Halaman Ikhtisar](#)
 - [Ringkasan laporan](#)
 - [Ringkasan penilaian](#)
 - [Halaman daftar isi](#)
 - [Halaman kontrol](#)
 - [Ringkasan kontrol](#)
 - [Bukti yang dikumpulkan](#)
 - [Halaman ringkasan bukti](#)
 - [Halaman detail bukti](#)
- [Memvalidasi laporan penilaian](#)
- [Sumber daya tambahan](#)

Memahami struktur folder laporan penilaian

Saat Anda mengunduh laporan penilaian, Audit Manager akan membuat folder zip. Ini berisi laporan penilaian Anda dan file bukti terkait di subfolder bersarang.

Folder zip disusun sebagai berikut:

- Folder penilaian (contoh:myAssessmentName-a1b2c3d4) — Folder root.
- Folder laporan penilaian (contoh:reportName-a1b2c3d4e5f6g7) - Subfolder tempat Anda dapat menemukan AssessmentReportSummary file.pdf, digest.txt, dan README.txt.
- Bukti dengan folder kontrol (contoh:controlName-a1b2c3d4e5f6g) — Subfolder yang mengelompokkan file bukti dengan kontrol terkait.
- Bukti oleh folder sumber data (contoh:CloudTrail,Security Hub CSPM) — Subfolder yang mengelompokkan file bukti berdasarkan tipe sumber data.
- Bukti berdasarkan folder tanggal (contoh:2022-07-01) — Subfolder yang mengelompokkan file bukti berdasarkan tanggal pengumpulan bukti.
- File bukti — File yang berisi rincian tentang potongan bukti individu.

Menavigasi laporan penilaian

Mulailah dengan membuka folder zip dan menavigasi satu tingkat ke bawah ke folder laporan penilaian. Di sini, Anda dapat menemukan laporan penilaian PDF dan file README.txt.

Anda dapat meninjau file README.txt untuk memahami struktur dan isi folder zip. Ini juga memberikan informasi referensi tentang konvensi penamaan untuk setiap file. Informasi ini dapat membantu Anda menavigasi langsung ke subfolder atau file bukti jika Anda mencari item tertentu.

Jika tidak, untuk menelusuri bukti dan menemukan informasi yang Anda butuhkan, buka PDF laporan penilaian. Ini memberi Anda gambaran tingkat tinggi dari laporan, dan ringkasan penilaian dari mana laporan itu dibuat.

Selanjutnya, gunakan daftar isi (TOC) untuk menjelajahi laporan. Anda dapat memilih kontrol hyperlink di TOC untuk melompat langsung ke ringkasan kontrol itu.

Ketika Anda siap untuk meninjau detail bukti untuk kontrol, Anda dapat melakukannya dengan memilih nama bukti hyperlink. Untuk bukti otomatis, hyperlink membuka file PDF baru dengan detail tentang bukti itu. Untuk bukti manual, hyperlink membawa Anda ke bucket S3 yang berisi bukti.

Tip

Navigasi breadcrumb di bagian atas setiap halaman menunjukkan lokasi Anda saat ini dalam laporan penilaian saat Anda menelusuri kontrol dan bukti. Pilih TOC hyperlink untuk menavigasi kembali ke TOC kapan saja.

Meninjau bagian dari laporan penilaian

Gunakan informasi berikut untuk mempelajari lebih lanjut tentang setiap bagian laporan penilaian.

Note

Ketika Anda melihat tanda hubung (-) di sebelah salah satu atribut di bagian berikut, ini menunjukkan bahwa nilai atribut itu adalah null, atau nilai tidak ada.

- [Halaman sampul](#)
- [Halaman Ikhtisar](#)
- [Halaman daftar isi](#)
- [Halaman kontrol](#)
- [Halaman ringkasan bukti](#)
- [Halaman detail bukti](#)

Halaman sampul

Halaman sampul berisi nama laporan penilaian. Ini juga menampilkan tanggal dan waktu laporan dibuat, bersama dengan ID akun pengguna yang membuat laporan.

Halaman sampul diformat sebagai berikut. Audit Manager menggantikan *placeholders* dengan informasi yang relevan dengan laporan Anda.

Assessment report name

Report generated on *MM/DD/YYYY* at *HH:MM:SS AM/PM UCT* by *AccountID*

Halaman Ikhtisar

Halaman ikhtisar memiliki dua bagian: ringkasan laporan itu sendiri, dan ringkasan penilaian yang dilaporkan.

Ringkasan laporan

Bagian ini merangkum laporan penilaian.

Nama	Deskripsi
Nama laporan	Nama laporan.
Deskripsi	Deskripsi yang dimasukkan oleh pemilik audit saat mereka membuat laporan.
Tanggal dihasilkan	Tanggal ketika laporan dibuat. Waktu diwakili dalam Coordinated Universal Time (UTC).
Total kontrol disertakan	Jumlah kontrol yang termasuk dalam laporan dan telah mengumpulkan bukti. Ini adalah bagian dari jumlah total kontrol dalam penilaian.
Akun AWS termasuk	Jumlah Akun AWS yang termasuk dalam laporan dan telah mengumpulkan bukti. Ini adalah bagian dari jumlah total Akun AWS dalam penilaian.
Pemilihan laporan penilaian	Jumlah item bukti yang dipilih untuk dimasukkan dalam laporan. Ini termasuk jumlah total masalah pemeriksaan kepatuhan yang ditemukan dalam laporan.

Ringkasan penilaian

Bagian ini merangkum penilaian yang terkait dengan laporan tersebut.

Nama	Deskripsi
Nama penilaian	Nama penilaian dari mana laporan itu dihasilkan.
Status	Status penilaian pada saat laporan dibuat.
Wilayah Penilai	Di Wilayah AWS mana penilaian dibuat.
Akun AWS dalam ruang lingkup	Daftar Akun AWS yang ada dalam lingkup penilaian.
Nama kerangka kerja	Nama kerangka kerja tempat penilaian dibuat.

Nama	Deskripsi
Pemilik audit	Pengguna atau peran pemilik audit penilaian.
Terakhir diperbarui	Tanggal ketika penilaian terakhir diperbarui. Waktu diwakili dalam UTC.

Halaman daftar isi

TOC menampilkan isi lengkap laporan penilaian. Isi dikelompokkan dan diatur berdasarkan set kontrol yang termasuk dalam penilaian. Kontrol terdaftar di bawah set kontrol masing-masing.

Pilih item apa pun dalam daftar isi untuk menavigasi langsung ke bagian laporan tersebut. Anda dapat memilih set kontrol atau langsung ke kontrol.

Halaman kontrol

Halaman kontrol memiliki dua bagian: ringkasan kontrol itu sendiri, dan ringkasan bukti yang dikumpulkan untuk kontrol.

Ringkasan kontrol

Bagian ini mencakup informasi berikut.

Nama	Deskripsi
Nama kontrol	Nama kontrol.
Deskripsi	Deskripsi kontrol.
Set kontrol	Nama set kontrol yang menjadi milik kontrol.
Menguji informasi	Prosedur pengujian yang direkomendasikan untuk kontrol ini.
Rencana aksi	Tindakan yang disarankan untuk dilakukan jika kontrol tidak terpenuhi.

Nama	Deskripsi
Pemilihan laporan penilaian	Jumlah item bukti yang terkait dengan kontrol ini yang dimasukkan dalam laporan penilaian. Ini termasuk jumlah masalah pemeriksaan kepatuhan yang ditemukan untuk bukti kontrol ini.

Bukti yang dikumpulkan

Bagian ini menunjukkan bukti yang dikumpulkan untuk kontrol. Bukti dikelompokkan berdasarkan folder, yang diatur dan diberi nama berdasarkan tanggal pengumpulan bukti. Di sebelah setiap nama folder bukti adalah jumlah total masalah pemeriksaan kepatuhan untuk folder itu.

Di bawah setiap nama folder bukti adalah daftar nama bukti hyperlink.

- Nama bukti otomatis dimulai dengan stempel waktu pengumpulan bukti, diikuti dengan kode layanan, nama acara (hingga 20 karakter), ID akun, dan ID unik 12 karakter unik.

Misalnya: 21-30-24_IAM_CreateUser_111122223333_a1b2c3d4e5f6

Untuk bukti otomatis, nama hyperlink membuka file PDF baru dengan ringkasan dan detail lebih lanjut.

- Nama bukti manual dimulai dengan stempel waktu unggahan bukti, diikuti dengan manual label, ID akun, dan ID unik 12 karakter. Mereka juga menyertakan 10 karakter pertama dari nama file, dan ekstensi file (hingga 10 karakter).

Misalnya: 00-00-00_manual_111122223333_a1b2c3d4e5f6_myimage.png

Untuk bukti manual, nama hyperlink membawa Anda ke bucket S3 yang berisi bukti itu.

Di sebelah setiap nama bukti adalah hasil pemeriksaan kepatuhan untuk item tersebut.

- Untuk bukti otomatis yang dikumpulkan dari AWS Security Hub CSPM atau AWS Config, hasil Compliant, Non-compliant, atau Inconclusive dilaporkan.
- Untuk bukti otomatis yang dikumpulkan dari AWS CloudTrail dan panggilan API, dan untuk semua bukti manual, hasil yang tidak meyakinkan ditampilkan.

Halaman ringkasan bukti

Halaman ringkasan bukti mencakup informasi berikut.

Nama	Deskripsi
ID	Pengidentifikasi unik untuk bukti.
Tanggal dikumpulkan	Tanggal ketika bukti dibuat atau diunggah.
Deskripsi	Deskripsi bukti, termasuk ID akun dan tipe sumber data.
Nama penilaian	Nama penilaian dari mana laporan itu dihasilkan.
Nama kerangka kerja	Nama kerangka kerja tempat penilaian dibuat.
Nama kontrol	Nama kontrol yang didukung bukti.
Kontrol nama set	Nama set kontrol yang dimiliki oleh kontrol terkait.
Deskripsi kontrol	Deskripsi kontrol yang didukung bukti.
Menguji informasi	Prosedur pengujian yang direkomendasikan untuk kontrol.
Rencana aksi	Tindakan yang disarankan untuk dilakukan jika kontrol tidak terpenuhi.
Wilayah AWS	Nama daerah yang terkait dengan bukti.
ID IAM	ARN dari pengguna atau peran yang terkait dengan bukti.
Akun AWS	Akun AWS ID yang terkait dengan bukti.
Layanan AWS	Nama Layanan AWS yang terkait dengan bukti.
Nama acara	Nama peristiwa bukti.
Waktu acara	Saat peristiwa bukti terjadi.

Nama	Deskripsi
Sumber data	Dari mana bukti dikumpulkan atau diunggah. Jenis sumber data dapat berupa AWS Config, Security Hub CSPM, panggilan AWS API CloudTrail, atau Manual.
Bukti berdasarkan jenis	Kategori bukti • Bukti pemeriksaan kepatuhan dikumpulkan dari AWS Config atau Security Hub CSPM. • Bukti aktivitas pengguna dikumpulkan dari CloudTrail log. • Bukti data konfigurasi dikumpulkan dari snapshot lainnya Layanan AWS. • Bukti manual adalah bukti bahwa Anda mengunggah secara manual.
Status pemeriksaan kepatuhan	Status evaluasi untuk bukti yang termasuk dalam kategori pemeriksaan kepatuhan. • Untuk bukti otomatis yang dikumpulkan dari AWS Security Hub CSPM atau AWS Config, hasil Compliant, Non-compliant, atau Inconclusive dilaporkan. • Untuk bukti otomatis yang dikumpulkan dari AWS CloudTrail dan panggilan API, dan untuk semua bukti manual, hasil yang tidak meyakinkan ditampilkan.

Halaman detail bukti

Halaman detail bukti menunjukkan nama bukti dan tabel detail bukti. Tabel ini memberikan rincian rinci dari setiap elemen bukti sehingga Anda dapat memahami data dan memvalidasi bahwa itu benar. Bergantung pada sumber data bukti, isi halaman detail bukti bervariasi.

 Tip

Navigasi breadcrumb di bagian atas setiap halaman menunjukkan lokasi Anda saat ini saat Anda menelusuri detail bukti. Pilih Ringkasan bukti untuk menavigasi kembali ke ringkasan bukti kapan saja.

Memvalidasi laporan penilaian

Saat Anda membuat laporan penilaian, Audit Manager menghasilkan checksum file laporan yang disebut `digest.txt`. Anda dapat menggunakan file ini untuk memvalidasi integritas laporan dan memastikan bahwa tidak ada bukti yang diubah setelah laporan dibuat. Ini berisi objek JSON dengan tanda tangan dan hash yang tidak valid jika ada bagian dari arsip laporan diubah.

Untuk memvalidasi integritas laporan penilaian, gunakan [ValidateAssessmentReportIntegrity](#) API yang disediakan oleh Audit Manager.

Sumber daya tambahan

Untuk menemukan jawaban atas pertanyaan dan masalah umum, lihat [Memecahkan masalah laporan penilaian](#) di bagian Pemecahan Masalah di panduan ini.

Pencari bukti

Pencari bukti menyediakan cara ampuh untuk mencari bukti di Audit Manager. Alih-alih menelusuri folder bukti yang sangat bersarang untuk menemukan apa yang Anda cari, Anda sekarang dapat menggunakan pencari bukti untuk menanyakan bukti Anda dengan cepat. Jika Anda menggunakan pencari bukti sebagai administrator yang didelegasikan, Anda dapat mencari bukti di semua akun anggota di organisasi Anda.

Dengan menggunakan kombinasi filter dan pengelompokan, Anda dapat secara progresif mempersempit cakupan permintaan pencarian Anda. Misalnya, jika Anda menginginkan tampilan tingkat tinggi kesehatan sistem Anda, lakukan pencarian luas dan filter berdasarkan penilaian, rentang tanggal, dan kepatuhan sumber daya. Jika tujuan Anda adalah memperbaiki sumber daya tertentu, Anda dapat melakukan pencarian sempit untuk menargetkan bukti untuk kontrol atau ID sumber daya tertentu. Setelah menentukan filter, Anda dapat mengelompokkan dan kemudian melihat pratinjau hasil pencarian yang cocok sebelum membuat laporan penilaian.

Untuk menggunakan pencari bukti, Anda harus mengaktifkan fitur ini dari setelan Audit Manager Anda.

Poin kunci

Memahami cara kerja pencari bukti dengan CloudTrail Lake

Pencari bukti menggunakan kemampuan [AWS CloudTrail Lake](#) dan penyimpanan Danau. Sebelum Anda mulai menggunakan pencari bukti, akan sangat membantu untuk memahami sedikit lebih banyak tentang cara kerja CloudTrail Danau.

CloudTrail Lake menggabungkan data ke dalam satu penyimpanan data peristiwa yang dapat dicari yang mendukung kueri SQL yang kuat. Ini berarti Anda dapat mencari data di seluruh organisasi Anda dan dalam rentang waktu khusus. Dengan pencari bukti, Anda dapat menggunakan fungsi pencarian ini secara langsung di konsol Audit Manager.

Saat Anda meminta untuk mengaktifkan pencari bukti, Manajer Audit membuat penyimpanan data peristiwa atas nama Anda. Setelah pencari bukti diaktifkan, semua bukti Manajer Audit Anda di masa mendatang dicerna ke penyimpanan data peristiwa yang tersedia untuk kueri pencarian pencari bukti. Setelah Anda mengaktifkan pencari bukti, kami juga mengisi kembali penyimpanan data peristiwa yang baru dibuat dengan data bukti Anda selama dua tahun terakhir. Jika Anda mengaktifkan pencari

bukti sebagai administrator yang didelegasikan, kami mengisi ulang data untuk semua akun anggota di organisasi Anda.

Semua data bukti Anda, baik yang diisi ulang atau baru, disimpan di penyimpanan data acara selama 2 tahun. Anda dapat mengubah periode penyimpanan default kapan saja. Untuk petunjuk, lihat [Memperbarui penyimpanan data peristiwa](#) di Panduan AWS CloudTrail Pengguna. Anda dapat menyimpan data di penyimpanan data acara hingga 7 tahun, atau 2.555 hari.

Note

Ketika data bukti baru ditambahkan ke penyimpanan data peristiwa, biaya CloudTrail Lake dikeluarkan untuk penyimpanan dan konsumsi data.

Untuk pertanyaan CloudTrail Danau, Anda membayar sambil pergi. Ini berarti bahwa untuk setiap kueri penelusuran yang Anda jalankan di pencari bukti, Anda dikenakan biaya untuk data yang dipindai.

Untuk informasi lebih lanjut tentang harga CloudTrail Danau, lihat [AWS CloudTrail harga](#).

Langkah selanjutnya

Untuk memulai, aktifkan pencari bukti dari pengaturan Manajer Audit Anda. Untuk petunjuk, lihat [Mengaktifkan pencari bukti](#).

Sumber daya tambahan

- [Mencari bukti di pencari bukti](#)
- [Melihat hasil di pencari bukti](#)
- [Opsis filter dan pengelompokan untuk pencari bukti](#)
- [Contoh kasus penggunaan untuk pencari bukti](#)
- [Memecahkan masalah pencari bukti](#)

Mencari bukti di pencari bukti

Anda dapat menggunakan pencari bukti untuk melakukan pencarian yang ditargetkan dan dengan cepat menampilkan bukti yang relevan untuk ditinjau.

Di halaman ini, Anda akan mempelajari cara memfilter pencarian berdasarkan kriteria seperti penilaian, rentang tanggal, status kepatuhan sumber daya, dan atribut tambahan. Menerapkan filter ini mempersempit ruang lingkup pencarian Anda hanya menjadi bukti yang Anda butuhkan. Anda juga dapat mengelompokkan hasil berdasarkan bidang tertentu untuk menganalisis pola dengan lebih baik.

Prasyarat

Pastikan Anda telah menyelesaikan langkah-langkah untuk mengaktifkan pencari bukti di setelan Audit Manager Anda. Untuk petunjuk, lihat [Mengaktifkan pencari bukti](#).

Selain itu, pastikan Anda memiliki izin untuk melakukan permintaan pencarian di pencari bukti. Untuk contoh kebijakan izin yang dapat Anda gunakan, lihat [Izinkan pengguna menjalankan kueri pencarian di pencari bukti](#).

Prosedur

Ikuti langkah-langkah ini untuk mencari bukti di konsol Audit Manager.

1. [Melakukan permintaan pencarian](#)
2. [Menghentikan kueri penelusuran yang sedang berlangsung \(opsional\)](#)
3. [Mengedit filter untuk permintaan pencarian Anda \(opsional\)](#)

Note

Anda juga dapat menggunakan CloudTrail API untuk menanyakan data bukti Anda. Untuk informasi selengkapnya, lihat [StartQuery](#) di dalam Referensi API AWS CloudTrail . Jika Anda lebih suka menggunakan AWS CLI, lihat [Memulai kueri](#) di Panduan AWS CloudTrail Pengguna.

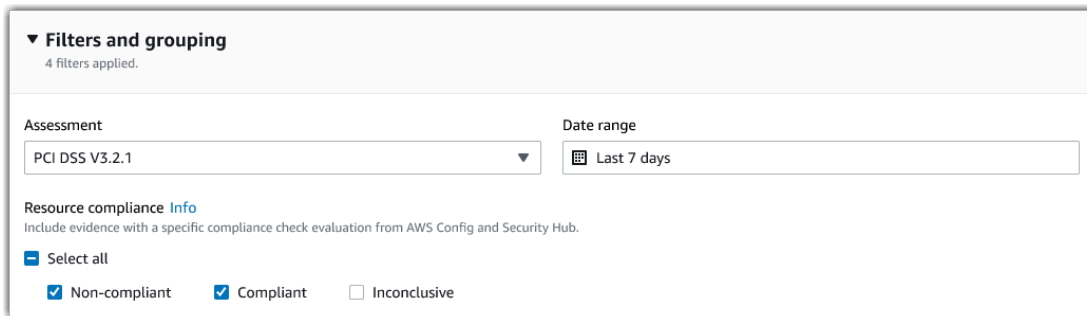
Melakukan permintaan pencarian

Ikuti langkah-langkah ini untuk melakukan permintaan pencarian di pencari bukti.

Untuk mencari bukti

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.

2. Di panel navigasi, pilih Pen cari bukti.
3. Selanjutnya, terapkan filter untuk mempersempit ruang lingkup pencarian Anda.
 - a. Untuk Penilaian, pilih penilaian.
 - b. Untuk Rentang tanggal, pilih rentang.
 - c. Untuk Kepatuhan sumber daya, pilih status evaluasi.



▼ **Filters and grouping**
4 filters applied.

Assessment
PCI DSS V3.2.1

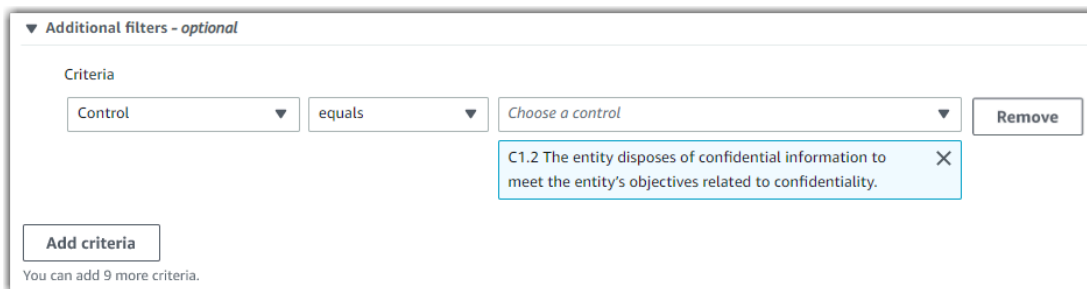
Date range
Last 7 days

Resource compliance [Info](#)
Include evidence with a specific compliance check evaluation from AWS Config and Security Hub.

☒ Select all

☒ Non-compliant ☒ Compliant ☐ Inconclusive

4. (Opsional) Pilih Filter tambahan - opsional untuk mempersempit pencarian lebih jauh.
 - a. Pilih Tambahkan kriteria, pilih kriteria, lalu pilih satu atau lebih nilai untuk kriteria tersebut.
 - b. Terus membangun lebih banyak filter dengan cara yang sama.
 - c. Untuk menghapus filter yang tidak diinginkan, pilih Hapus.



▼ **Additional filters - optional**

Criteria

Control equals Choose a control Remove

C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality. X

Add criteria

You can add 9 more criteria.

5. Di bawah Pengelompokan, tentukan apakah Anda ingin mengelompokkan hasil pencarian.
 - a. Jika Anda ingin mengelompokkan hasil, pilih nilai untuk mengelompokkan hasil.
 - b. Jika Anda tidak ingin mengelompokkan hasilnya, lanjutkan ke langkah 6.

Grouping Info
You can group your search results to make them easier to navigate.

☒ **Group results**
Sort the search results into groups, based on a specific value that you choose. Generating a grouped list of results incurs an additional charge.

☐ **Don't group results**
Return an ungrouped list of all search results.

Group by
You can group your search results by any of these values.

Resource type ▼

6. Pilih Cari.

Clear filters Search

Pencarian Anda mungkin memakan waktu beberapa menit, tergantung pada jumlah data bukti yang Anda miliki. Jangan ragu untuk menavigasi jauh dari pencari bukti saat pencarian sedang berlangsung. Bilah flash memberi tahu Anda ketika hasil pencarian siap.

Menghentikan kueri penelusuran

Jika Anda ingin menghentikan permintaan pencarian karena alasan apa pun, ikuti langkah-langkah ini.

Note

Menghentikan kueri penelusuran masih dapat mengakibatkan biaya. Anda akan dikenakan biaya untuk jumlah data bukti yang dipindai sebelum Anda menghentikan kueri penelusuran. Setelah dihentikan, Anda dapat melihat hasil parsial yang dikembalikan.

Untuk menghentikan kueri penelusuran yang sedang berlangsung

1. Di bilah flash progres biru di bagian atas layar, pilih Hentikan pencarian.

⌚ Your search is **in progress** and might take a few minutes to complete. When it's done, you can view the search results on the [Evidence finder](#) page. Stop search

2. (Opsional) Tinjau hasil paruh yang dikembalikan sebelum Anda menghentikan kueri penelusuran.
 - a. Jika Anda berada di halaman pencari bukti, hasil parsial ditampilkan di layar.
 - b. Jika Anda menavigasi jauh dari pencari bukti, pilih Lihat hasil paruh di bilah flash konfirmasi hijau.

✓ Your search has stopped successfully. You can now view the partial results that were returned before you stopped the search.

[View partial results](#)

Mengedit filter pencarian

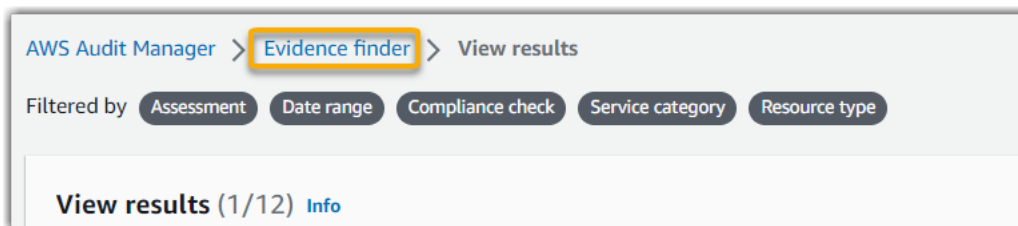
Ikuti langkah-langkah ini untuk kembali ke permintaan pencarian terbaru Anda dan sesuaikan filter sesuai kebutuhan.

Note

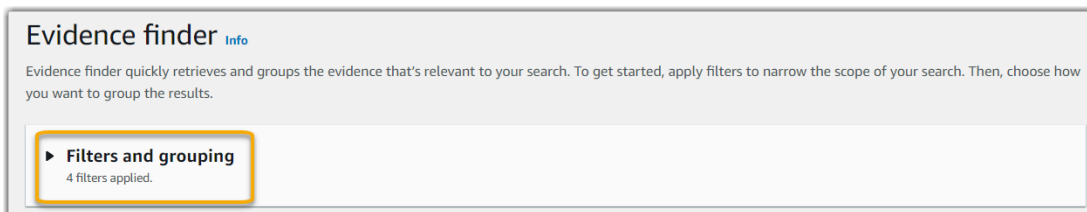
Saat Anda mengedit filter dan memilih **Cari**, ini memulai kueri pencarian baru.

Cara mengedit kueri penelusuran terbaru

1. Dari halaman **Lihat hasil**, pilih **Pencari bukti** dari menu navigasi breadcrumb.



2. Pilih **Filter dan pengelompokan** untuk memperluas pilihan filter.



3. Selanjutnya, edit filter Anda atau mulai pencarian baru.
 - a. Untuk mengedit filter, sesuaikan atau hapus filter saat ini dan pemilihan pengelompokan.
 - b. Untuk memulai dari awal, pilih **Hapus filter** dan terapkan filter dan pemilihan pengelompokan pilihan Anda.



4. Setelah selesai, pilih Cari.



Langkah selanjutnya

Setelah pencarian Anda selesai, Anda dapat melihat hasil yang sesuai dengan kriteria pencarian Anda. Untuk petunjuk, lihat [Melihat hasil di pencari bukti](#).

Sumber daya tambahan

- [Opsis filter dan pengelompokan untuk pencari bukti](#)
- [Contoh kasus penggunaan untuk pencari bukti](#)
- [Memecahkan masalah pencari bukti](#)

Melihat hasil di pencari bukti

Setelah pencarian Anda selesai, Anda dapat melihat hasil yang sesuai dengan kriteria pencarian Anda.

Perlu diingat bahwa beberapa sumber daya dapat dinilai selama pengumpulan bukti. Akibatnya, bukti dapat mencakup satu atau lebih sumber daya terkait. Dalam pencari bukti, hasil ditampilkan pada tingkat sumber daya, dengan satu baris untuk setiap sumber daya. Anda dapat melihat ringkasan setiap sumber daya tanpa meninggalkan halaman.

Setelah meninjau hasil pencarian, Anda dapat membuat laporan penilaian yang menyertakan bukti tersebut. Anda juga dapat mengekspor hasil penelusuran ke dalam file nilai yang dipisahkan koma (CSV).

Important

Kami menyarankan agar Anda tetap membuka pencari bukti sampai Anda selesai menjelajahi hasil pencarian Anda. Hasil pencarian Anda akan dibuang saat Anda menavigasi jauh dari tabel Lihat Hasil. Jika perlu, Anda dapat [melihat hasil terbaru Anda](#) di CloudTrail konsol di <https://console.aws.amazon.com/cloudtrail/>. Di sini, hasil permintaan pencarian Anda

dipertahankan selama tujuh hari. Namun, perlu diingat bahwa Anda tidak dapat membuat laporan penilaian dari hasil penelusuran di CloudTrail konsol.

Prasyarat

Prosedur berikut mengasumsikan bahwa Anda sudah mengikuti langkah-langkah untuk [melakukan pencarian](#) di pencari bukti.

Prosedur

Ikuti langkah-langkah ini untuk melihat hasil pencarian Anda di pencari bukti.

Tugas

- [Langkah 1. Melihat hasil yang dikelompokkan](#)
- [Langkah 2. Melihat hasil pencarian](#)
 - [Mengelola preferensi tampilan Anda](#)
 - [Pratinjau ringkasan sumber daya](#)

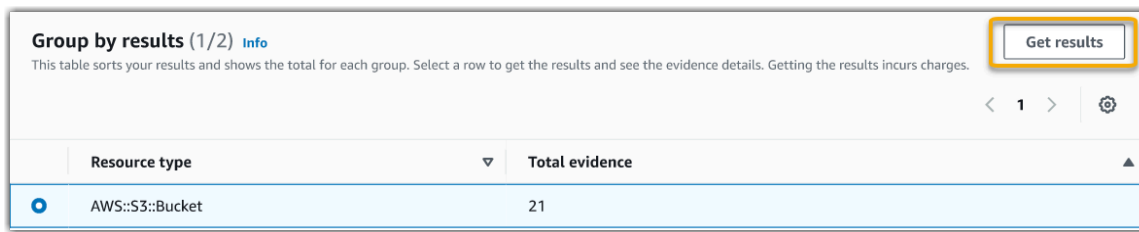
Langkah 1. Melihat hasil yang dikelompokkan

Jika Anda mengelompokkan hasil Anda, Anda dapat meninjau pengelompokan sebelum Anda menyelami lebih dalam bukti.

Note

Jika Anda tidak mengelompokkan hasil, pencari bukti tidak menampilkan tabel Grup berdasarkan hasil. Sebagai gantinya, Anda dibawa langsung ke tabel Lihat hasil.

Gunakan tabel Grup berdasarkan hasil untuk mempelajari luasnya bukti yang cocok dan bagaimana hal itu didistribusikan di dimensi tertentu. Hasil dikelompokkan berdasarkan nilai yang Anda pilih. Misalnya, jika Anda dikelompokkan berdasarkan jenis Sumber daya, tabel menunjukkan daftar jenis AWS sumber daya. Kolom bukti total menunjukkan jumlah hasil pencocokan untuk setiap jenis sumber daya.



Untuk mendapatkan hasil untuk grup

1. Dari tabel Kelompokkan berdasarkan hasil, pilih baris untuk hasil yang ingin Anda dapatkan.
2. Pilih Dapatkan hasil. Ini memulai kueri penelusuran baru, dan mengarahkan Anda ke tabel Lihat hasil tempat Anda dapat melihat hasil untuk grup tersebut.

Langkah 2. Melihat hasil pencarian

Tabel Lihat hasil menampilkan hasil pencarian Anda. Dari sini, Anda dapat mengelola preferensi tampilan dan pratinjau ringkasan sumber daya.

Mengelola preferensi tampilan Anda

Preferensi tampilan Anda mengontrol apa yang Anda lihat di halaman hasil.

Untuk mengelola preferensi tampilan Anda

1. Pilih ikon pengaturan (#) di bagian atas tabel Lihat hasil.
2. Tinjau dan ubah pengaturan berikut sesuai kebutuhan:

Pengaturan	Deskripsi
Pilih kolom tabel yang terlihat	Gunakan opsi sakelar untuk mengubah kolom mana yang ditampilkan.
Ukuran halaman	Pilih tombol radio untuk menentukan berapa banyak hasil yang ditampilkan pada setiap halaman.
Bungkus teks	Pilih kotak centang untuk membungkus baris teks yang panjang untuk keterbacaan yang lebih baik.

3. Pilih Konfirmasi untuk menyimpan preferensi Anda.

Pratinjau ringkasan sumber daya

Anda dapat melihat pratinjau sumber daya terkait untuk bukti yang cocok dengan permintaan pencarian Anda. Ini membantu Anda menentukan apakah kueri penelusuran mengembalikan hasil yang diinginkan, atau jika Anda perlu menyesuaikan filter dan menjalankan kembali kueri penelusuran.

Perlu diingat bahwa bukti dapat memiliki satu atau lebih sumber daya terkait. Pencari bukti menunjukkan hasil pada tingkat sumber daya (dengan satu baris untuk setiap sumber daya).

Note

Pencari bukti mengembalikan hasil untuk bukti otomatis dan manual. Namun, Anda hanya dapat melihat ringkasan sumber daya untuk bukti otomatis. Ini karena Audit Manager tidak melakukan penilaian sumber daya untuk bukti manual, dan sebagai hasilnya, tidak ada ringkasan sumber daya yang tersedia.

Untuk melihat detail tentang bukti manual, pilih nama bukti untuk membuka halaman detail bukti. Jika Anda membuat laporan penilaian dari hasil pencari bukti Anda, detail bukti manual disertakan dalam laporan penilaian.

Untuk melihat ringkasan sumber daya

1. Pilih tombol radio di sebelah hasil. Ini membuka panel ringkasan sumber daya pada halaman saat ini.
2. (Opsional) Untuk melihat detail lengkap dari bukti terkait, pilih nama bukti.
3. (Opsional) Gunakan garis horizontal (=) untuk menyeret dan mengubah ukuran panel ringkasan sumber daya.
4. Pilih (x) untuk menutup panel ringkasan sumber daya.

Evidence	Resource ARN	Resource compliance	Date and time
☐ 22615e944-a8b2-4cb0-85e4-d853ea94347b	arn:aws:iam:us-west-1:[:policyName]	Non-compliant	August 10, 2022, 7:30 (UTC+00:00)
☒ 99615e944-a8b2-4cb0-85e4-d853ea94350d	arn:aws:cloudtrail:us-west-1:[:trail/AWSOrganizationMaster]	Compliant	August 10, 2022, 7:30 (UTC+00:00)
☐ 99615e944-a8b2-4cb0-85e4-d853ea94350d	arn:aws:cloudtrail:us-west-1:[:trail/]	Compliant	August 10, 2022, 7:30 (UTC+00:00)

99615e944-a8b2-4cb0-85e4-d853ea94350d

Resource summary

Resource ARN arn:aws:iam:us-west-1:[:policyName]	Data source type AWS Config	Assessment PCI DSS V3.2.1
Resource Type AWS::S3::Bucket	Data source mapping S3_BUCKET_PUBLIC_READ_PROHIBITED	Control domain Identity and access management
Resource compliance Non-compliant	Account ID [redacted]	Control 7.2.1 Confirm that access control systems are in place on all system components.
Date and time August 10, 2022, 7:30 (UTC+00:00)		

Langkah selanjutnya

Setelah meninjau hasil penelusuran, Anda dapat membuat laporan penilaian dari mereka atau mengekspornya sebagai file CSV. Untuk petunjuk, lihat [Mengekspor hasil pencarian Anda dari pencari bukti](#).

Sumber daya tambahan

- [Opsi filter dan pengelompokan untuk pencari bukti](#)
- [Contoh kasus penggunaan untuk pencari bukti](#)
- [Memecahkan masalah pencari bukti](#)

Mengekspor hasil pencarian Anda dari pencari bukti

Setelah meninjau hasil penelusuran, Anda dapat membuat laporan penilaian berdasarkan hasil tersebut. Atau, Anda dapat mengekspor hasil pencarian pencari bukti Anda dalam file CSV.

Prasyarat

Prosedur berikut mengasumsikan bahwa Anda sudah mengikuti langkah-langkah untuk [melakukan pencarian](#) dan men [injau hasil pencarian Anda](#) di pencari bukti.

Prosedur

Daftar Isi

- [Membuat laporan penilaian dari hasil pencarian Anda](#)
- [Mengekspor hasil pencarian Anda ke file CSV](#)
 - [Melihat hasil setelah Anda mengekspornya](#)

Membuat laporan penilaian dari hasil pencarian Anda

Setelah puas dengan hasil pencarian, Anda dapat membuat laporan penilaian.

Untuk membuat laporan penilaian dari hasil pencarian Anda

1. Di bagian atas tabel Lihat hasil, pilih Buat laporan penilaian.
2. Masukkan nama dan deskripsi untuk laporan penilaian Anda, dan tinjau detail laporan penilaian.
3. Pilih Buat laporan penilaian.

Diperlukan beberapa menit untuk membuat laporan penilaian Anda. Anda dapat menjauh dari pencari bukti saat ini terjadi, dan pemberitahuan keberhasilan hijau akan mengkonfirmasi kapan laporan siap. Anda kemudian dapat pergi ke pusat unduhan Audit Manager dan [mengunduh laporan penilaian Anda](#).

Note

Audit Manager menghasilkan laporan satu kali hanya menggunakan bukti dari hasil pencarian. Laporan ini tidak menyertakan bukti apa pun yang [ditambahkan secara manual ke laporan dari halaman penilaian](#).

Batasan berlaku untuk berapa banyak bukti yang dapat dimasukkan dalam laporan penilaian. Untuk informasi selengkapnya, lihat [Memecahkan masalah pencari bukti](#).

Mengekspor hasil pencarian Anda ke file CSV

Anda mungkin memerlukan versi portabel dari hasil pencarian pencari bukti Anda. Jika demikian, Anda dapat mengekspor hasil pencarian Anda ke file CSV.

Setelah Anda mengekspor hasil penelusuran, file CSV tersedia di pusat unduhan Audit Manager selama tujuh hari. Salinan file CSV juga dikirimkan ke bucket S3 pilihan Anda, yang dikenal sebagai tujuan ekspor. File CSV Anda tetap tersedia di bucket ini sampai Anda menghapus file tersebut.

Audit Manager menggunakan [fungsionalitas](#) CloudTrail Lake untuk mengekspor dan mengirimkan file CSV dari pencari bukti. Faktor-faktor berikut menentukan cara kerja proses ekspor CSV:

- Semua hasil pencarian Anda disertakan dalam file CSV. Jika Anda hanya ingin menyertakan hasil pencarian tertentu, kami sarankan Anda [mengedit filter pencarian Anda](#). Dengan cara ini, Anda dapat mempersempit hasil Anda untuk menargetkan hanya bukti yang ingin Anda ekspor.
- File CSV diekspor dalam format GZIP terkompresi. Nama file CSV default adalah `queryID/result.csv.gz`, di mana `queryID` ID kueri penelusuran Anda.
- Ukuran file maksimum untuk ekspor CSV adalah 1 TB. Jika Anda mengekspor lebih dari 1 TB data, hasil Anda dibagi menjadi lebih dari satu file. Setiap file CSV diberi nama `result_number.csv.gz`. Jumlah file CSV yang Anda dapatkan tergantung pada ukuran total hasil pencarian Anda. Misalnya, mengekspor 2 TB data memberi Anda dua file hasil kueri: `result_1.csv.gz` dan `result_2.csv.gz`.
- Selain file CSV, file tanda JSON dikirim ke bucket S3 Anda. File ini bertindak sebagai checksum untuk memverifikasi bahwa informasi dalam file CSV akurat. Untuk mempelajari selengkapnya, lihat struktur file [CloudTrail tanda](#) tangan di Panduan AWS CloudTrail Pengembang. Untuk menentukan apakah hasil kueri dimodifikasi, dihapus, atau tidak berubah setelah dikirimkan, Anda dapat menggunakan validasi integritas CloudTrail hasil kueri. Untuk petunjuk, lihat [Mem validasi hasil kueri yang disimpan](#) di Panduan AWS CloudTrail Pengembang.

Note

Tanggapan teks bukti manual saat ini tidak termasuk dalam pratinjau pencari bukti atau ekspor CSV. Untuk melihat data respons teks, pilih nama bukti manual di hasil pencari bukti Anda untuk membuka halaman detail bukti. Jika Anda perlu melihat data respons teks di luar konsol Audit Manager, sebaiknya buat laporan penilaian dari hasil pencari bukti. Semua detail bukti manual, termasuk tanggapan teks, disertakan dalam laporan penilaian.

Mengekspor hasil Anda untuk pertama kalinya

Ikuti langkah-langkah ini untuk mengekspor hasil pencarian Anda untuk pertama kalinya. Prosedur ini memberi Anda opsi untuk menentukan tujuan ekspor default untuk semua ekspor Anda di masa mendatang. Jika Anda tidak ingin menyimpan tujuan ekspor default sekarang, Anda dapat melakukannya nanti dengan [memperbarui pengaturan tujuan ekspor Anda](#).

Important

Sebelum memulai, pastikan Anda memiliki bucket S3 yang tersedia untuk digunakan sebagai tujuan ekspor Anda. Anda dapat menggunakan salah satu bucket S3 yang sudah ada, atau Anda dapat [membuat bucket baru di Amazon S3](#). Untuk keamanan dan kinerja yang optimal, sebaiknya gunakan bucket S3 di AWS akun dan wilayah yang sama dengan penilaian Anda. Selain itu, bucket S3 Anda harus memiliki kebijakan izin yang diperlukan CloudTrail untuk memungkinkan menulis file ekspor ke dalamnya. Lebih khusus lagi, kebijakan bucket harus menyertakan `s3:PutObject` tindakan dan bucket ARN, dan daftar CloudTrail sebagai prinsipal layanan. Kami memberikan [contoh kebijakan izin](#) yang dapat Anda gunakan. Untuk petunjuk tentang cara melampirkan kebijakan ini ke bucket S3 Anda, lihat Men [ambahkan kebijakan bucket menggunakan konsol Amazon S3](#).

Untuk tips lebih lanjut, lihat [Kiat konfigurasi untuk tujuan ekspor Anda](#). Jika Anda mengalami masalah saat mengekspor file CSV, lihat [csv-exports](#).

Untuk mengekspor hasil pencarian Anda (pengalaman dijalankan pertama)

1. Di bagian atas tabel Lihat hasil, pilih Ekspor CSV.
2. Tentukan bucket S3 tempat Anda ingin mengekspor file Anda.
 - Pilih Browse S3 untuk memilih dari daftar bucket Anda.
 - Atau, Anda dapat memasukkan URI bucket dalam format ini: **s3://bucketname/prefix**

Tip

Agar bucket tujuan tetap teratur, Anda dapat membuat folder opsional untuk ekspor CSV Anda. Untuk melakukannya, tambahkan garis miring (/) dan awalan ke nilai di kotak URI Sumber Daya (misalnya, **/evidenceFinderExports**). Audit Manager kemudian menyertakan awalan ini ketika menambahkan file CSV ke bucket, dan Amazon

S3 menghasilkan jalur yang ditentukan oleh awalan. Untuk informasi selengkapnya tentang awalan di Amazon S3, lihat [Mengatur objek di konsol Amazon S3](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

3. (Opsional) Jika Anda tidak ingin menyimpan bucket ini sebagai tujuan ekspor default, kosongkan kotak centang yang mengatakan Simpan bucket ini sebagai tujuan ekspor default di pengaturan pencari bukti saya.
4. Pilih Ekspor.

Mengekspor hasil setelah Anda menyimpan tujuan ekspor

Setelah Anda menyimpan bucket S3 default sebagai tujuan ekspor default, Anda dapat mengikuti langkah-langkah ini ke depan.

Untuk mengekspor hasil pencarian Anda (setelah Anda menyimpan tujuan ekspor default)

1. Di bagian atas tabel Lihat hasil, pilih Ekspor CSV.
2. Pada prompt yang muncul, tinjau bucket S3 default tempat file yang diekspor Anda akan disimpan.
 - a. (Opsional) Untuk terus menggunakan bucket ini dan menyembunyikan pesan ini ke depan, centang kotak Jangan ingatkan saya lagi.
 - b. (Opsional) Untuk mengubah bucket ini, ikuti prosedur untuk [memperbarui pengaturan tujuan ekspor Anda](#).
3. Pilih Konfirmasi.

Bergantung pada berapa banyak data yang Anda ekspor, proses ekspor dapat memakan waktu beberapa menit untuk menyelesaikannya. Anda dapat menavigasi jauh dari pencari bukti saat ekspor sedang berlangsung. Saat Anda menjauh dari pencari bukti, pencarian Anda dihentikan dan hasil pencarian Anda dibuang di konsol. Namun, proses ekspor CSV berlanjut di latar belakang. File CSV akan berisi kumpulan lengkap hasil pencarian yang cocok dengan kueri Anda.

Melihat hasil setelah Anda mengekspornya

Untuk menemukan file CSV Anda dan memeriksa statusnya, buka Manajer Audit [Pusat unduhan Audit Manager](#). Ketika file yang diekspor sudah siap, Anda dapat [mengunduh file CSV Anda](#) dari pusat unduhan.

Anda juga dapat menemukan dan mengunduh file CSV dari bucket S3 tujuan ekspor Anda.

Untuk menemukan file CSV Anda dan menandatangani file di konsol Amazon S3

1. Buka [konsol Amazon S3](#).
2. Pilih bucket tujuan ekspor yang Anda tentukan saat mengekspor file CSV.
3. Navigasi melalui hierarki objek hingga Anda menemukan file CSV dan file tanda. File CSV memiliki `.csv.gz` ekstensi dan file tanda memiliki `.json` ekstensi.

Anda akan menavigasi melalui hierarki objek yang mirip dengan contoh berikut, tetapi dengan nama bucket tujuan ekspor yang berbeda, ID akun, tanggal, dan ID kueri.

```
All Buckets
  Export_Destination_Bucket_Name
    AWSLogs
      Account_ID;
        CloudTrail-Lake
          Query
            YYYY
              MM
                DD
                  Query_ID
```

Sumber daya tambahan

- [Memecahkan masalah pencari bukti](#)
- [Mengkonfigurasi tujuan ekspor default Anda untuk pencari bukti](#)

Opsi filter dan pengelompokan untuk pencari bukti

Di halaman ini, Anda dapat melihat daftar opsi filter dan pengelompokan yang tersedia untuk Anda gunakan di pencari bukti.

Referensi filter

Anda dapat menggunakan filter berikut untuk menemukan bukti yang cocok dengan kriteria tertentu, seperti penilaian, kontrol, atau Layanan AWS.

Topik

- [Filter yang diperlukan](#)
- [Filter tambahan \(opsional\)](#)
- [Menggabungkan filter](#)

Filter yang diperlukan

Gunakan filter ini untuk memulai dengan ikhtisar tingkat tinggi dari bukti dalam penilaian.

Nama filter	Deskripsi	Catatan
Penilaian	Mengembalikan bukti untuk penilaian tertentu.	Anda dapat memfilter berdasarkan satu penilaian saja.
Rentang tanggal	Mengembalikan bukti untuk periode waktu tertentu.	Baik, Anda dapat menggunakan rentang Relatif untuk menentukan rentang yang relatif terhadap tanggal hari ini (misalnya, Last 30 days). Atau, Anda dapat menggunakan rentang Absolute untuk menentukan rentang tanggal tertentu (misalnya, June 27th - July 4th).
Kepatuhan sumber daya	Mengembalikan sumber daya dengan evaluasi pemeriksaan kepatuhan tertentu.	Audit Manager mengumpulkan bukti pemeriksaan an kepatuhan untuk kontrol yang menggunakan AWS Config dan Security Hub CSPM sebagai jenis sumber data. Beberapa sumber daya dapat dinilai selama pengumpulan bukti. Akibatnya, satu bukti pemeriksaan kepatuhan dapat mencakup satu atau lebih sumber daya. Anda dapat menggunakan filter ini untuk menjelajahi status kepatuhan di tingkat sumber daya. Anda dapat memilih satu atau beberapa opsi berikut: • Non-compliant— Filter ini menemukan sumber daya dengan masalah pemeriksaan kepatuhan

Nama filter	Deskripsi	Catatan
		. Ini terjadi jika Security Hub melaporkan hasil Gagal, atau jika AWS Config melaporkan Non-compliant hasilnya. • Sesuai — Filter ini menemukan sumber daya yang tidak memiliki masalah pemeriksaan kepatuhan. Ini terjadi jika Security Hub CSPM melaporkan hasil Pass, atau jika AWS Config melaporkan hasil Compliant. • Tidak meyakinkan — Filter ini menemukan sumber daya yang pemeriksaan kepatuhannya tidak tersedia atau tidak dapat diterapkan. Ini terjadi jika sumber daya menggunakan AWS Config atau Security Hub CSPM sebagai tipe sumber data yang mendasarinya, tetapi layanan tersebut tidak diaktifkan. Ini juga terjadi jika sumber daya menggunakan tipe sumber data dasar yang tidak mendukung pemeriksaan kepatuhan (seperti bukti manual, panggilan AWS API, atau CloudTrail).

Filter tambahan (opsional)

Gunakan filter ini untuk mempersempit cakupan permintaan pencarian Anda. Misalnya, gunakan Layanan untuk melihat semua bukti yang terkait dengan Amazon S3. Gunakan tipe Resource untuk fokus hanya pada bucket S3. Atau, gunakan Resource ARN untuk menargetkan bucket S3 tertentu.

Anda dapat membuat filter tambahan menggunakan satu atau lebih kriteria berikut.

Nama Kriteria	Deskripsi	Kapan menggunakan kriteria ini
ID Akun	Jelajahi ke bawah Akun AWS.	Gunakan kriteria ini untuk menemukan bukti yang terkait dengan tertentu Akun AWS.

Nama Kriteria	Deskripsi	Kapan menggunakan kriteria ini
Kontrol	Jelajahi dengan nama kontrol.	Gunakan kriteria ini untuk menemukan bukti yang terkait dengan kontrol tertentu.
Domain kontrol	Jelajahi berdasarkan domain kontrol.	Gunakan kriteria ini untuk fokus pada bidang subjek tertentu saat Anda mempersiapkan audit. Anda dapat memfilter berdasarkan domain kontrol jika Anda menanyakan penilaian yang dibuat dari kerangka kerja standar. Contoh domain kontrol termasuk keamanan jaringan, manajemen identitas dan akses, dan perlindungan data. Beberapa domain kontrol mungkin ditandai sebagai Uusi any setelah transisi Manajer Audit ke kumpulan domain kontrol baru yang disediakan oleh Katalog AWS Kontrol. Untuk informasi selengkapnya, lihat Saya melihat bahwa domain kontrol ditandai sebagai “usang”. Apa artinya ini?.
Jenis sumber data	Jelajahi berdasarkan jenis sumber data.	Gunakan kriteria ini untuk fokus pada sumber data tertentu. Tetapkan nilai Manual untuk menemukan bukti yang Anda unggah secara manual. Jika tidak, Anda dapat memfilter bukti otomatis berdasarkan dari mana asalnya (misalnya ,AWS Config,CloudTrail ,Security Hub CSPM, atauAWS API calls).
Nama acara	Jelajahi berdasarkan nama acara.	Gunakan kriteria ini untuk fokus pada peristiwa tertentu yang terkait dengan bukti. Peristiwa adalah catatan aktivitas dalam sebuah Akun AWS. Misalnya, Anda dapat mencari nama panggilan API, seperti AttachRolePolicy operasi IAM yang digunakan untuk mengonfigurasi izin. Atau, cari CloudTrail kata kunci, seperti ConsoleLogin peristiwa yang dicatat CloudTrail saat pengguna masuk ke akun Anda.

Nama Kriteria	Deskripsi	Kapan menggunakan kriteria ini
Sumber daya ARN	Jelajahi berdasarkan Nama Sumber Daya Amazon (ARN).	Gunakan kriteria ini untuk menemukan bukti yang terkait dengan AWS sumber daya tertentu.
Tipe sumber daya	Jelajahi berdasarkan jenis sumber daya.	Gunakan kriteria ini untuk fokus pada jenis sumber daya yang sedang dinilai, seperti instans Amazon EC2 atau bucket S3.
Layanan	Jelajahi dengan Layanan AWS nama.	Gunakan kriteria ini untuk menemukan bukti yang terkait dengan tertentu Layanan AWS, seperti Amazon EC2, Amazon S3, atau AWS Config.
Kategori layanan	Jelajahi berdasarkan Layanan AWS kategori.	Gunakan kriteria ini untuk fokus pada kategori tertentu Layanan AWS. Contohnya termasuk keamanan, identitas dan kepatuhan, database, dan penyimpanan.

Menggabungkan filter

Perilaku kriteria

Bila Anda menentukan lebih dari satu kriteria, Audit Manager menerapkan AND operator ke pilihan Anda. Ini berarti bahwa semua kriteria dikelompokkan menjadi satu kueri, dan hasilnya harus cocok dengan semua kriteria gabungan.

Contoh

Dalam pengaturan filter berikut, pencari bukti mengembalikan sumber daya yang tidak sesuai dari 7 hari terakhir untuk penilaian yang dipanggil **MySOC2Assessment**. Selain itu, hasilnya berhubungan dengan kebijakan IAM dan kontrol yang ditentukan.

Assessment: MySOC2Assessment | Date range: Last 7 days

Resource compliance [Info](#)
Include evidence with a specific compliance check evaluation from AWS Config and Security Hub.

☒ Select all
☒ Non-compliant ☐ Compliant ☐ Inconclusive

▼ Additional filters - optional

Criteria

Control equals Choose a control [Remove](#)
 7.2.1 Confirm that access control systems are in place on all system components. [×](#)

and Resource type contains [Remove](#)
 AWS::IAM::Policy [×](#)

[Add criteria](#)

Perilaku nilai kriteria

Bila Anda menentukan lebih dari satu nilai kriteria, nilai-nilai tersebut ditautkan dengan OR operator. Pencari bukti mengembalikan hasil yang cocok dengan salah satu nilai kriteria ini.

Contoh

Dalam pengaturan filter berikut, pencari bukti mengembalikan hasil pencarian yang berasal dari AWS CloudTrail, AWS Config, atau AWS Security Hub CSPM.

and Data source type equals Choose a data source type [Remove](#)

AWS CloudTrail [×](#) AWS Config [×](#) AWS SecurityHub [×](#)

Referensi pengelompokan

Anda dapat mengelompokkan hasil pencarian Anda untuk navigasi yang lebih cepat. Pengelompokan menunjukkan luasnya hasil pencarian Anda, dan bagaimana mereka didistribusikan di dimensi tertentu.

Anda dapat menggunakan salah satu grup berikut berdasarkan nilai.

Kelompokkan oleh	Deskripsi
ID Akun	Kelompokkan hasil berdasarkan Akun AWS.
Kontrol	Kelompokkan hasil berdasarkan nama kontrol.

Kelompokkan oleh	Deskripsi
Jenis sumber data	Kelompokkan hasil berdasarkan jenis sumber data dari mana bukti berasal.
Nama acara	Kelompokkan hasil berdasarkan nama acara.
Sumber daya ARN	Kelompokkan hasil berdasarkan Nama Sumber Daya Amazon (ARN).
Tipe sumber daya	Kelompokkan hasil berdasarkan jenis sumber daya.
Layanan	Kelompokkan hasil berdasarkan Layanan AWS nama.
Kategori layanan	Hasil grup berdasarkan Layanan AWS kategori.

Contoh kasus penggunaan untuk pencari bukti

Pencari bukti dapat membantu Anda dengan beberapa kasus penggunaan. Halaman ini memberikan beberapa contoh dan menyarankan filter pencarian yang dapat Anda gunakan di setiap skenario.

Topik

- [Kasus penggunaan 1: Temukan bukti yang tidak sesuai dan atur delegasi](#)
- [Kasus penggunaan 2: Identifikasi bukti yang sesuai](#)
- [Kasus penggunaan 3: Lakukan pratinjau cepat sumber bukti](#)

Kasus penggunaan 1: Temukan bukti yang tidak sesuai dan atur delegasi

Kasus penggunaan ini sangat ideal jika Anda seorang petugas kepatuhan, petugas perlindungan data, atau profesional GRC yang mengawasi persiapan audit.

Saat Anda memantau postur kepatuhan untuk organisasi Anda, Anda mungkin mengandalkan tim mitra untuk membantu Anda memperbaiki masalah. Anda dapat menggunakan pencari bukti untuk membantu Anda mengatur pekerjaan Anda untuk tim mitra Anda.

Dengan menerapkan filter, Anda dapat fokus pada bukti untuk satu area pada satu waktu. Selain itu, Anda juga dapat tetap selaras dengan tanggung jawab dan ruang lingkup setiap tim mitra yang

bekerja dengan Anda. Dengan melakukan pencarian yang ditargetkan dengan cara ini, Anda dapat menggunakan hasil pencarian untuk mengidentifikasi apa yang sebenarnya perlu diperbaiki di setiap area subjek. Anda kemudian dapat mendelegasikan bukti yang tidak sesuai itu ke tim mitra terkait untuk remediasi.

Untuk alur kerja ini, ikuti langkah-langkah untuk [mencari bukti](#). Gunakan filter berikut untuk menemukan bukti yang tidak sesuai.

```
Assessment | <assessment name>  
Date range | <date range>  
Resource compliance | Non-compliant
```

Selanjutnya, terapkan filter tambahan untuk area yang Anda fokuskan. Misalnya, gunakan filter kategori Layanan untuk menemukan sumber daya yang tidak sesuai yang terkait dengan IAM. Kemudian, bagikan hasil tersebut dengan tim yang memiliki sumber daya IAM untuk organisasi Anda. Atau, jika Anda menanyakan penilaian yang dibuat dari kerangka kerja standar, Anda dapat menggunakan filter domain Kontrol untuk menemukan bukti yang tidak sesuai yang terkait dengan domain manajemen identitas dan akses.

```
Control domain | <domain that you're focusing on>  
or  
Service category | <Layanan AWS category that you're focusing on>
```

Setelah Anda menemukan bukti yang Anda butuhkan, ikuti langkah-langkah untuk membuat laporan penilaian dari hasil pencarian Anda. Untuk petunjuk, lihat [Membuat laporan penilaian dari hasil pencarian Anda](#). Anda dapat membagikan laporan ini dengan tim mitra Anda, yang dapat menggunakannya sebagai daftar Periksa remediasi.

Kasus penggunaan 2: Identifikasi bukti yang sesuai

Kasus penggunaan ini sangat ideal jika Anda bekerja di SecOps, IT/DevOps, atau peran lain yang memiliki dan memperbaiki aset cloud.

Sebagai bagian dari audit, Anda mungkin diminta untuk memperbaiki masalah dengan sumber daya yang Anda miliki. Setelah Anda melakukan pekerjaan ini, Anda dapat menggunakan pencari bukti untuk memvalidasi bahwa sumber daya Anda sesuai.

Untuk alur kerja ini, ikuti langkah-langkah untuk [mencari bukti](#). Gunakan filter berikut untuk menemukan bukti yang sesuai.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Compliant
```

Selanjutnya, terapkan filter tambahan untuk hanya menampilkan bukti yang menjadi tanggung jawab Anda. Tergantung pada ruang lingkup kepemilikan Anda, buat pencarian sesuai target yang diperlukan. Contoh filter berikut diurutkan dari yang paling luas hingga yang paling tepat. Pilih opsi yang sesuai untuk Anda, dan ganti *<placeholder text>* dengan nilai-nilai Anda sendiri.

```
Control domain | <a subject area that you're responsible for>
Service category | <a category of Layanan AWS that you own>
Service | <a specific Layanan AWS that you own>
Resource type | <a collection of resources that you own>
Resource ARN | <a specific resource that you own>
```

Jika Anda bertanggung jawab atas beberapa contoh dari kriteria yang sama (misalnya, Anda memiliki beberapa Layanan AWS), Anda dapat mengelom [pokkan hasil](#) berdasarkan nilai tersebut. Ini memberi Anda total kecocokan bukti untuk masing-masing Layanan AWS. Anda kemudian bisa mendapatkan hasil untuk layanan yang Anda miliki.

Kasus penggunaan 3: Lakukan pratinjau cepat sumber bukti

Kasus penggunaan ini sangat ideal untuk semua pelanggan Audit Manager.

Sebelumnya, itu memakan waktu untuk meninjau detail bukti individu. Jika Anda ingin melihat pratinjau bukti, Anda harus pergi langsung ke penilaian itu, lalu menavigasi melalui folder bukti yang sangat bersarang. Sekarang, pencari bukti menyediakan cara mudah untuk melihat informasi ini. Untuk setiap item bukti yang cocok dengan permintaan pencarian Anda, Anda dapat melihat pratinjau sumber daya individu untuk bukti tersebut.

Untuk memulai, ikuti langkah-langkah untuk [mencari bukti](#). Kemudian, pilih tombol radio di sebelah hasil untuk melihat ringkasan sumber daya di halaman saat ini. Anda dapat melihat pratinjau setiap sumber daya individu yang berhubungan dengan item bukti. Untuk melihat detail bukti lengkap untuk sumber daya apa pun, pilih nama bukti. Untuk informasi selengkapnya, lihat [Pratinjau ringkasan sumber daya](#).

Evidence 	Resource ARN	Resource compliance	Date and time
 22615e944-a8b2-4cb0-85e4-d853ea94347b	 <code>arn:aws:iam:us-west-1:██████████:policyName</code>	 Non-compliant	August 10, 2022, 7:30 (UTC+00:00)
 99615e944-a8b2-4cb0-85e4-d853ea94350d	 <code>arn:aws:cloudtrail:us-west-1:██████████:trail/AWSOrganizationMaster</code>	 Compliant	August 10, 2022, 7:30 (UTC+00:00)
 99615e944-a8b2-4cb0-85e4-d853ea94350d	 <code>arn:aws:cloudtrail:us-west-1:██████████:trail/</code>	 Compliant	August 10, 2022, 7:30 (UTC+00:00)

99615e944-a8b2-4cb0-85e4-d853ea94350d

Resource summary

Resource ARN  <code>arn:aws:iam:us-west-1:██████████:policyName</code>	Data source type AWS Config	Assessment PCI DSS V3.2.1 
Resource Type AWS::S3::Bucket	Data source mapping S3_BUCKET_PUBLIC_READ_PROHIBITED	Control domain Identity and access management
Resource compliance  Non-compliant	Account ID ██████████	Control 7.2.1 Confirm that access control systems are in place on all system components.
Date and time August 10, 2022, 7:30 (UTC+00:00)		

Pusat unduhan Audit Manager

Pusat unduhan adalah tempat Anda dapat menemukan dan mengelola semua file Audit Manager yang dapat diunduh. Saat Anda membuat laporan penilaian atau mengekspor hasil pencarian dari pencari bukti, file akan muncul di pusat unduhan.

Daftar Isi

- [Menjelajahi pusat unduhan](#)
- [Mengunduh file](#)
- [Menghapus file](#)
- [Sumber daya tambahan](#)

Menjelajahi pusat unduhan

Ikuti langkah-langkah ini untuk menelusuri file Anda di pusat unduhan.

Untuk menemukan file di pusat unduhan

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.
2. Di panel navigasi kiri, pilih Pusat unduhan.
3. Pilih tab Laporan penilaian untuk melihat laporan penilaian yang tersedia untuk diunduh.
 - Tab ini menampilkan laporan penilaian yang telah Anda buat. Laporan penilaian tetap tersedia di pusat unduhan hingga Anda menghapusnya.
 - Untuk melihat status terbaru laporan penilaian Anda, pilih ikon penyegaran (↻) untuk memuat ulang tabel. Setiap baris dalam tabel laporan penilaian menunjukkan nama laporan, tanggal pembuatannya, dan salah satu status berikut:

Status	Deskripsi
Sedang berlangsung	Audit Manager membuat laporan penilaian.
Siap	Laporan penilaian tersedia untuk Anda unduh.

Status	Deskripsi
Kesalahan	Laporan penilaian gagal dihasilkan. Dalam hal ini, Audit Manager menampilkan pesan yang menjelaskan kesalahan. Untuk informasi tentang cara mengatasi kesalahan ini, lihat Memecahkan masalah laporan penilaian.

4. Pilih tab Ekspor untuk melihat ekspor CSV yang tersedia untuk diunduh.

- Tab ini menunjukkan hasil pencarian pencari bukti yang Anda ekspor dalam tujuh hari terakhir. File CSV dihapus dari pusat unduhan setelah tujuh hari, tetapi tetap tersedia di bucket S3 [tujuan ekspor](#) Anda. Untuk petunjuk tentang cara menemukan ekspor CSV pencari bukti di bucket tujuan S3 Anda, lihat. [Melihat hasil setelah Anda mengekspornya](#)
- Untuk melihat status terbaru ekspor CSV Anda, pilih ikon refresh (↺) untuk memuat ulang tabel. Setiap baris dalam tabel ekspor menunjukkan nama file, tanggal ekspornya, dan salah satu status berikut:

Status	Deskripsi
Sedang berlangsung	Audit Manager sedang mempersiapkan file CSV.
Siap	Ekspor berhasil dan file tersedia untuk Anda unduh.
Kesalahan	Ekspor gagal. Dalam hal ini, Audit Manager menampilkan pesan yang menjelaskan kesalahan. Untuk informasi tentang cara mengatasi kesalahan ini, lihat csv-exports.

 Note

Perlu diingat bahwa tab ekspor mungkin juga menampilkan file CSV untuk kueri yang Anda jalankan langsung di Lake. AWS CloudTrail Ini termasuk kueri yang dibuat di CloudTrail konsol atau menggunakan CloudTrail API. CloudTrail ekspor muncul di tab ini jika Anda menanyakan penyimpanan data peristiwa Audit Manager, dan Anda memilih untuk menyimpan hasilnya ke Amazon S3.

Mengunduh file

Ikuti langkah-langkah ini untuk mengunduh file dari pusat unduhan.

Untuk mengunduh file

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.
2. Di panel navigasi kiri, pilih Pusat unduhan.
3. Pilih tab Laporan penilaian atau tab Ekspor.
4. Pilih file yang ingin Anda unduh, dan pilih Unduh.

Untuk petunjuk tentang cara mengunduh file langsung dari bucket tujuan S3, lihat [Mengunduh objek](#) di Panduan Pengguna Amazon Simple Storage Service (Amazon S3).

Menghapus file

Ikuti langkah-langkah ini untuk menghapus laporan penilaian apa pun yang tidak lagi Anda perlukan di pusat unduhan.

Note

Menghapus ekspor CSV dari pusat unduhan saat ini tidak didukung. Ekspor CSV secara otomatis dihapus dari pusat unduhan setelah tujuh hari.

Untuk menghapus laporan penilaian

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.
2. Di panel navigasi kiri, pilih Pusat unduhan.
3. Pilih tab Laporan penilaian.
4. Pilih laporan penilaian yang ingin Anda hapus, lalu pilih Hapus.

Jika ingin menghapus laporan penilaian atau ekspor CSV dari bucket tujuan S3, sebaiknya selesaikan tugas ini secara langsung di Amazon S3. Untuk petunjuk, lihat [Menghapus objek Amazon S3 di Panduan Pengguna Amazon Simple Storage Service \(Amazon S3\)](#) Simple Storage Service (Amazon S3).

Sumber daya tambahan

- [Mengkonfigurasi tujuan ekspor default Anda untuk pencari bukti](#)
- [Mengkonfigurasi tujuan laporan penilaian default](#)
- [Memecahkan masalah laporan penilaian](#)
- [Memecahkan masalah ekspor CSV](#)
- [Mengunduh objek dari Amazon S3](#)
- [Menghapus objek Amazon S3](#)

Menggunakan pustaka kerangka kerja untuk mengelola kerangka kerja di AWS Audit Manager

Anda dapat menemukan dan mengelola kerangka kerja di pustaka kerangka kerja di AWS Audit Manager.

Kerangka kerja menentukan kontrol mana yang diuji di lingkungan selama periode waktu tertentu. Ini mendefinisikan kontrol dan pemetaan sumber data mereka untuk standar kepatuhan atau peraturan tertentu. Ini juga digunakan untuk menyusun dan mengotomatiskan penilaian Manajer Audit. Anda dapat menggunakan kerangka kerja sebagai titik awal untuk mengaudit Layanan AWS penggunaan Anda dan mulai mengotomatiskan pengumpulan bukti.

Poin kunci

Di perpustakaan kerangka kerja, kerangka kerja diatur ke dalam kategori berikut.

- **Kerangka kerja standar** adalah kerangka kerja bawaan yang AWS menyediakan. Kerangka kerja ini didasarkan pada praktik AWS terbaik untuk standar dan peraturan kepatuhan yang berbeda, seperti GDPR dan HIPAA. Kerangka kerja standar mencakup kontrol yang diatur ke dalam kumpulan kontrol berdasarkan standar kepatuhan atau peraturan yang didukung kerangka kerja.

Anda dapat melihat isi kerangka kerja standar, tetapi Anda tidak dapat mengedit atau menghapusnya. Namun, Anda dapat membuat salinan kerangka kerja standar yang dapat diedit untuk membuat yang baru untuk memenuhi persyaratan spesifik Anda.

- **Kerangka kerja khusus** adalah kerangka kerja yang Anda buat. Anda dapat membuat kerangka kerja khusus dari awal, atau dengan membuat salinan kerangka kerja yang ada yang dapat diedit. Anda dapat menggunakan kerangka kerja khusus untuk mengatur kontrol ke dalam kumpulan kontrol dengan cara yang memenuhi persyaratan spesifik Anda.

Anda dapat membuat penilaian dari kerangka standar atau kerangka kerja khusus.

Note

AWS Audit Manager membantu mengumpulkan bukti yang relevan untuk memverifikasi kepatuhan terhadap standar dan peraturan kepatuhan tertentu. Namun, itu tidak menilai kepatuhan Anda sendiri. Bukti yang dikumpulkan oleh AWS Audit Manager karena itu

mungkin tidak mencakup semua informasi tentang AWS penggunaan Anda yang diperlukan untuk audit. AWS Audit Manager bukan pengganti penasihat hukum atau pakar kepatuhan.

Sumber daya tambahan

Untuk membuat dan mengelola kerangka kerja di Audit Manager, ikuti prosedur yang diuraikan di sini.

- [Menemukan kerangka kerja yang tersedia di AWS Audit Manager](#)
- [Meninjau kerangka kerja di AWS Audit Manager](#)
- [Membuat kerangka kerja khusus di AWS Audit Manager](#)
 - [Membuat kerangka kerja khusus dari awal di AWS Audit Manager](#)
 - [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#)
- [Mengedit kerangka kerja khusus di AWS Audit Manager](#)
- [Menghapus kerangka kerja khusus di AWS Audit Manager](#)
- [Berbagi kerangka kerja khusus di AWS Audit Manager](#)
 - [Kerangka kerja berbagi konsep dan terminologi](#)
 - [Mengirim permintaan untuk berbagi kerangka kerja khusus di AWS Audit Manager](#)
 - [Menanggapi permintaan berbagi di AWS Audit Manager](#)
 - [Menghapus permintaan berbagi di AWS Audit Manager](#)
- [Kerangka kerja yang didukung di AWS Audit Manager](#)

Menemukan kerangka kerja yang tersedia di AWS Audit Manager

Anda dapat menemukan semua kerangka kerja yang tersedia di halaman pustaka Framework di konsol Audit Manager.

Anda juga dapat melihat semua kerangka kerja yang tersedia menggunakan API Audit Manager atau AWS Command Line Interface (AWS CLI).

Prasyarat

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk melihat kerangka kerja di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah

[AWSAuditManagerAdministratorAccess](#) dan [izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Audit Manager console

Untuk melihat kerangka kerja yang tersedia di konsol Audit Manager

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi kiri, pilih pustaka Framework.
3. Pilih tab Kerangka standar atau tab kerangka kerja khusus untuk menelusuri kerangka kerja standar dan kustom yang tersedia.

AWS CLI

Untuk melihat kerangka kerja yang tersedia di AWS CLI

Untuk melihat kerangka kerja di Audit Manager, gunakan [perintah](#) `list-assessment-framework` dan tentukan a. `--framework-type` Entah, Anda dapat mengambil daftar kerangka kerja standar. Atau, Anda dapat mengambil daftar kerangka kerja khusus.

```
aws auditmanager list-assessment-frameworks --framework-type Standard
```

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

Audit Manager API

Untuk melihat kerangka kerja yang tersedia menggunakan API

Gunakan [ListAssessmentFrameworks](#) operasi dan tentukan [FrameworkType](#). Entah, Anda dapat mengembalikan daftar kerangka kerja standar. Atau, Anda dapat mengembalikan daftar kerangka kerja khusus.

Untuk informasi selengkapnya, pilih salah satu tautan sebelumnya untuk membaca lebih lanjut di Refer AWS Audit Manager ensi API. Ini termasuk informasi tentang cara menggunakan `ListAssessmentFrameworks` operasi dan parameter di salah satu SDK khusus bahasa AWS .

Langkah selanjutnya

Saat Anda siap untuk menjelajahi detail kerangka kerja, ikuti langkah-langkah di [Meninjau kerangka kerja di AWS Audit Manager](#). Halaman ini akan memandu Anda melalui detail kerangka kerja dan menjelaskan informasi yang Anda lihat di sana.

Dari halaman perpustakaan kerangka kerja, Anda juga dapat [membuat](#), [mengedit](#), [menghapus](#), atau [berbagi](#) kerangka kerja khusus.

Sumber daya tambahan

Untuk solusi untuk masalah kerangka kerja di Audit Manager, lihat [Memecahkan masalah kerangka kerja](#).

Meninjau kerangka kerja di AWS Audit Manager

Anda dapat meninjau detail kerangka kerja menggunakan konsol Audit Manager, API Manajer Audit, atau AWS Command Line Interface (AWS CLI).

Prasyarat

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk melihat kerangka kerja di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Audit Manager console

Untuk melihat detail kerangka kerja di konsol Audit Manager

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi kiri, pilih pustaka Framework untuk melihat daftar kerangka kerja yang tersedia.
3. Pilih tab Kerangka standar atau tab kerangka kerja khusus untuk menelusuri kerangka kerja yang tersedia.
4. Pilih nama kerangka kerja untuk membukanya.

5. Tinjau detail kerangka kerja menggunakan informasi berikut sebagai referensi.

Bagian detail kerangka kerja

Bagian ini memberikan ikhtisar kerangka kerja. Di bagian ini, Anda dapat meninjau informasi berikut:

Nama	Deskripsi
Deskripsi	Deskripsi kerangka kerja, jika ada yang disediakan.
Jenis kerangka kerja	Menentukan apakah kerangka kerja adalah kerangka kerja standar atau kerangka kerja khusus.
Jenis kepatuhan	Standar kepatuhan atau peraturan yang didukung kerangka kerja.

Jika Anda melihat kerangka kerja khusus, Anda juga dapat melihat detail berikut:

Nama	Deskripsi
Dibuat oleh	Akun yang membuat kerangka kerja khusus.
Tanggal dibuat	Tanggal ketika kerangka kerja khusus dibuat.
Terakhir diperbarui	Tanggal ketika kerangka kerja ini terakhir diedit.

Tab kontrol

Tab ini mencantumkan kontrol dalam kerangka kerja, dikelompokkan berdasarkan kumpulan kontrol. Pada tab ini, Anda dapat meninjau informasi berikut:

Nama	Deskripsi
Kontrol dikelompokkan berdasarkan kumpulan kontrol	Pilih ikon tampilan pohon untuk melihat kontrol yang dimiliki setiap kumpulan kontrol.

Nama	Deskripsi
Jenis	Menentukan apakah kontrol adalah kontrol standar atau kontrol kustom.
Sumber data	Menentukan sumber data tempat Audit Manager mengumpulkan bukti untuk kontrol kerangka kerja tersebut.

Tab tag

Tab ini mencantumkan tag yang terkait dengan kerangka kerja. Pada tab ini, Anda dapat meninjau informasi berikut:

Nama	Deskripsi
Kunci	Kunci tag (misalnya, standar kepatuhan, peraturan, atau kategori).
Nilai	Nilai tanda.

AWS CLI

Untuk melihat detail kerangka kerja di AWS CLI

1. Untuk mengidentifikasi kerangka [kerja yang ingin Anda tinjau, jalankan](#) perintah list-assessment framework dan tentukan a. --framework-type Entah, Anda dapat mengambil daftar kerangka kerja standar. Atau, Anda dapat mengambil daftar kerangka kerja khusus.

Dalam contoh berikut, ganti *placeholder text* dengan salah satu Custom atau Standard.

```
aws auditmanager list-assessment-frameworks --framework-type Custom/Standard
```

Respons mengembalikan daftar kerangka kerja. Temukan kerangka kerja yang ingin Anda tinjau, dan catat ID kerangka kerja dan Nama Sumber Daya Amazon (ARN).

2. Untuk mendapatkan detail kerangka kerja, jalankan [perintah](#) get-assessment framework dan tentukan. --framework-id

Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri.

```
aws auditmanager get-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

 Tip

Detail kerangka kerja dikembalikan dalam format JSON. Untuk memahami data ini, lihat keluaran [get-assessment framework](#) di Referensi Perintah. AWS CLI

3. Untuk melihat tag untuk kerangka kerja, gunakan [perintah](#) `list-tags-for-resource` dan tentukan untuk kerangka kerja. `--resource-arn`

Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri:

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:assessmentFramework/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Untuk informasi selengkapnya tentang tag di Audit Manager, lihat Men [andai AWS Audit Manager sumber daya](#).

Audit Manager API

Untuk melihat detail kerangka kerja menggunakan API

1. Untuk mengidentifikasi kerangka kerja yang ingin Anda tinjau, gunakan [ListAssessmentFrameworks](#) operasi dan tentukan [FrameworkType](#). Entah, Anda dapat mengembalikan daftar kerangka kerja standar. Atau, Anda dapat mengembalikan daftar kerangka kerja khusus.

Dari tanggapan, temukan kerangka kerja yang ingin Anda tinjau dan catat ID kerangka kerja dan Nama Sumber Daya Amazon (ARN).

2. Untuk mendapatkan detail kerangka kerja, gunakan [GetAssessmentFramework](#) operasi. Dalam permintaan, tentukan [frameworkId](#) yang Anda dapatkan dari langkah 1.

 Tip

Detail kerangka kerja dikembalikan dalam format JSON. Untuk memahami data ini, lihat Elem [GetAssessmentFramework en Resp](#) on di Refer AWS Audit Manager ensi API.

3. Untuk melihat tag untuk kerangka kerja, gunakan [ListTagsForResource](#) operasi. Dalam permintaan, tentukan kerangka kerja [Belajar](#) yang Anda dapatkan dari langkah 1.

Untuk informasi selengkapnya tentang tag di Audit Manager, lihat Men [andai AWS Audit Manager sumber daya](#).

Untuk informasi selengkapnya tentang operasi API ini, pilih salah satu tautan di prosedur sebelumnya untuk membaca lebih lanjut di Refer AWS Audit Manager ensi API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasa AWS .

Langkah selanjutnya

Dari halaman detail kerangka kerja, Anda dapat [membuat penilaian dari kerangka kerja](#) atau [membuat salinan kerangka](#) kerja yang dapat diedit.

Jika Anda meninjau kerangka kerja khusus, Anda juga dapat [mengedit](#), [menghapus](#), atau [berbagi](#) kerangka kerja.

Sumber daya tambahan

- [Pada halaman detail kerangka kerja kustom saya, saya diminta untuk membuat ulang kerangka kerja khusus saya](#)
- [Saya tidak dapat membuat salinan kerangka kerja khusus saya](#)

Membuat kerangka kerja khusus di AWS Audit Manager

Anda dapat menggunakan kerangka kerja khusus untuk mengatur kontrol ke dalam kumpulan kontrol dengan cara yang memenuhi persyaratan spesifik Anda.

Poin kunci

Saat membuat kerangka kerja khusus di Audit Manager, Anda memiliki dua metode untuk dipilih:

1. Membuat kerangka kerja khusus dari awal - Ini memberi Anda fleksibilitas untuk memulai dengan batu tulis yang bersih dan menentukan setiap aspek kerangka kerja sesuai dengan spesifikasi Anda. Pendekatan ini sangat bermanfaat ketika persyaratan Anda menyimpang secara signifikan dari kerangka kerja standar yang ada, atau ketika Anda perlu memasukkan set kontrol eksklusif khusus untuk organisasi Anda.
2. Membuat salinan kerangka kerja yang ada yang dapat diedit - Pendekatan ini memungkinkan Anda untuk memanfaatkan struktur dan konten kerangka kerja yang ada sambil memberikan kebebasan untuk menyesuaikannya sesuai dengan kebutuhan spesifik Anda. Dengan memulai dengan fondasi yang mapan, Anda dapat merampingkan proses membangun kerangka kerja khusus Anda, memfokuskan upaya Anda untuk menyesuaikannya dengan persyaratan unik organisasi Anda.

Terlepas dari pendekatan yang Anda pilih, membuat kerangka kerja khusus melibatkan serangkaian langkah seperti menentukan detail kerangka kerja, mendefinisikan kumpulan kontrol, dan meninjau kerangka kerja sebelum menyelesaikan pembuatannya. Sepanjang proses ini, Anda dapat menggabungkan kumpulan kontrol spesifik organisasi Anda, memastikan bahwa kerangka kerja khusus secara akurat mencerminkan persyaratan GRC Anda.

Sumber daya tambahan

Untuk petunjuk tentang cara membuat kerangka kerja khusus, lihat sumber daya berikut.

- [Membuat kerangka kerja khusus dari awal di AWS Audit Manager](#)
- [Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager](#)

Membuat kerangka kerja khusus dari awal di AWS Audit Manager

Jika persyaratan kepatuhan organisasi Anda tidak selaras dengan kerangka kerja standar pra-bangun yang tersedia di AWS Audit Manager, Anda dapat membuat kerangka kerja khusus Anda sendiri dari awal sebagai gantinya.

Halaman ini menguraikan langkah-langkah untuk membuat kerangka kerja khusus yang disesuaikan dengan kebutuhan spesifik Anda.

Prasyarat

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk membuat kerangka kerja khusus di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Tugas

- [Langkah 1: Tentukan detail kerangka kerja](#)
- [Langkah 2: Tentukan set kontrol](#)
- [Langkah 3: Tinjau dan buat kerangka kerja](#)

Langkah 1: Tentukan detail kerangka kerja

Mulailah dengan menentukan detail tentang kerangka kerja kustom Anda.

Untuk menentukan detail kerangka kerja

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi kiri, pilih pustaka Framework dan kemudian pilih Buat kerangka kerja khusus.
3. Di bawah Detail Framework, masukkan nama, jenis kepatuhan (opsional), dan deskripsi untuk kerangka kerja Anda (juga opsional). Memasukkan jenis kepatuhan seperti PCI_DSS atau GDPR berarti Anda dapat menggunakan kata kunci ini untuk mencari kerangka kerja Anda nanti.
4. Di bawah Tag, pilih Tambahkan tag baru untuk mengaitkan tag dengan kerangka kerja Anda. Anda dapat menentukan kunci dan nilai untuk setiap tag. Kunci tag adalah wajib. Anda dapat menggunakannya sebagai kriteria pencarian saat mencari kerangka kerja ini di perpustakaan kerangka kerja.
5. Pilih Berikutnya.

Langkah 2: Tentukan set kontrol

Selanjutnya, Anda menentukan kontrol mana yang ingin Anda tambahkan ke kerangka kerja Anda dan bagaimana Anda ingin mengaturnya. Mulailah dengan menambahkan kumpulan kontrol ke kerangka kerja, lalu tambahkan kontrol ke kumpulan kontrol.

Note

Saat Anda menggunakan AWS Audit Manager konsol untuk membuat kerangka kerja khusus, Anda dapat menambahkan hingga 10 set kontrol untuk setiap kerangka kerja.

Saat Anda menggunakan Audit Manager API untuk membuat kerangka kerja khusus, Anda dapat membuat lebih dari 10 set kontrol. Untuk menambahkan lebih banyak kumpulan kontrol daripada yang diizinkan konsol saat ini, gunakan [CreateAssessmentFramework](#) API yang disediakan Audit Manager.

Untuk menentukan kumpulan kontrol

1. Di bawah Nama set kontrol, masukkan nama untuk kumpulan kontrol Anda.
2. Di bawah Tam bah kontrol, gunakan daftar tar ik-turun Jenis kontrol untuk memilih salah satu dari dua jenis kontrol: Kontrol standar atau Kontrol khusus.
3. Berdasarkan opsi yang Anda pilih pada langkah sebelumnya, daftar kontrol standar atau kontrol khusus ditampilkan. Pilih satu atau lebih kontrol dan pilih Tambahkan ke kumpulan kontrol.
4. Di jendela pop-up yang muncul, pilih Tambahkan ke kumpulan kontrol.
5. Tinjau kontrol yang muncul di daftar kontrol yang dipilih.
 - Untuk menambahkan lebih banyak kontrol, ulangi langkah 2—4.
 - Untuk menghapus kontrol yang tidak diinginkan, pilih satu atau beberapa kontrol dan pilih H apus kontrol.
6. Untuk menambahkan kumpulan kontrol baru, pilih Tam bah kumpulan kontrol.
7. Untuk menghapus kumpulan kontrol yang tidak diinginkan, pilih H apus kumpulan kontrol.
8. Setelah Anda selesai menambahkan set kontrol dan kontrol, pilih Ber ikutnya.

Langkah 3: Tinjau dan buat kerangka kerja

Tinjau informasi untuk kerangka kerja Anda. Untuk mengubah informasi untuk satu langkah, pilih Edit.

Setelah selesai, pilih **Buat kerangka kerja khusus**.

Langkah selanjutnya

Setelah Anda membuat kerangka kustom baru, Anda dapat membuat penilaian dari kerangka kerja Anda. Untuk informasi selengkapnya, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk meninjau kembali kerangka kerja khusus Anda di kemudian hari, lihat [Menemukan kerangka kerja yang tersedia di AWS Audit Manager](#). Anda dapat mengikuti langkah-langkah ini untuk menemukan kerangka kerja kustom Anda sehingga Anda kemudian dapat melihat, mengedit, berbagi, atau menghapusnya.

Sumber daya tambahan

Untuk solusi untuk masalah kerangka kerja di Audit Manager, lihat [Memecahkan masalah kerangka kerja](#).

Membuat salinan kerangka kerja yang ada yang dapat diedit di AWS Audit Manager

Alih-alih membuat kerangka kerja khusus dari awal, Anda dapat menggunakan kerangka kerja yang ada sebagai titik awal dan membuat salinan yang dapat diedit. Ketika Anda melakukan ini, kerangka kerja yang ada tetap berada di pustaka kerangka kerja, dan kerangka kerja khusus baru dibuat dengan pengaturan spesifik Anda.

Anda dapat membuat salinan yang dapat diedit dari kerangka kerja yang ada. Ini bisa berupa kerangka kerja standar atau kerangka kerja khusus.

Prasyarat

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk membuat kerangka kerja khusus di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Tugas

- [Langkah 1: Tentukan detail kerangka kerja](#)
- [Langkah 2: Tentukan set kontrol](#)

- [Langkah 3: Tinjau dan buat kerangka kerja](#)

Langkah 1: Tentukan detail kerangka kerja

Semua detail kerangka kerja, kecuali tag, dibawa dari kerangka asli. Tinjau dan ubah detail ini sesuai kebutuhan.

Untuk menentukan detail kerangka kerja

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi kiri, pilih pustaka Framework.
3. Pilih kerangka kerja yang ingin Anda gunakan sebagai titik awal, pilih Buat kerangka kerja khusus, lalu pilih Buat salinan.
4. Di jendela pop-up yang muncul, masukkan nama untuk kerangka kustom baru dan pilih Lanjutkan.
5. Di bawah Detail Framework, tinjau nama, jenis kepatuhan, dan deskripsi untuk kerangka kerja Anda, dan ubah sesuai kebutuhan. Jenis kepatuhan harus menunjukkan standar kepatuhan atau peraturan yang terkait dengan kerangka kerja Anda. Anda dapat menggunakan kata kunci ini untuk mencari kerangka kerja Anda.
6. Di bawah Tag, pilih Tambahkan tag baru untuk mengaitkan tag dengan kerangka kerja Anda. Anda dapat menentukan kunci dan nilai untuk setiap tag. Kunci tag adalah wajib dan dapat digunakan sebagai kriteria pencarian saat Anda mencari kerangka kerja ini di perpustakaan kerangka kerja.
7. Pilih Berikutnya.

Langkah 2: Tentukan set kontrol

Kumpulan kontrol dibawa dari kerangka kerja asli. Ubah konfigurasi saat ini dengan menambahkan lebih banyak kontrol atau menghapus kontrol yang ada sesuai kebutuhan.

Note

Saat Anda menggunakan konsol Audit Manager untuk membuat kerangka kerja khusus, Anda dapat menambahkan hingga 10 set kontrol untuk setiap kerangka kerja. Saat Anda menggunakan Audit Manager API untuk membuat kerangka kerja khusus, Anda dapat menambahkan lebih dari 10 set kontrol. Untuk menambahkan lebih banyak kumpulan

kontrol daripada yang diizinkan konsol saat ini, gunakan [CreateAssessmentFramework](#) API yang disediakan Audit Manager.

Untuk menentukan kumpulan kontrol

1. Di bawah nama set kontrol, ubah nama kumpulan kontrol sesuai kebutuhan.
2. Di bawah Tambah kontrol, tambahkan kontrol baru dengan menggunakan daftar dropdown untuk memilih salah satu dari dua jenis kontrol: Kontrol standar atau Kontrol khusus.
3. Berdasarkan opsi yang Anda pilih pada langkah sebelumnya, daftar kontrol standar atau kontrol khusus ditampilkan. Pilih satu atau lebih kontrol dan pilih Tambahkan ke kumpulan kontrol.
4. Di jendela pop-up yang muncul, pilih Tambahkan ke kumpulan kontrol.
5. Tinjau kontrol yang muncul di daftar kontrol yang dipilih.
 - Untuk menambahkan lebih banyak kontrol, ulangi langkah 2—4.
 - Untuk menghapus kontrol yang tidak diinginkan, pilih satu atau beberapa kontrol dan pilih Hapus kontrol.
6. Untuk menambahkan kumpulan kontrol baru ke kerangka kerja, pilih Tambahkan set kontrol.
7. Untuk menghapus kumpulan kontrol yang tidak diinginkan, pilih Hapus kumpulan kontrol.
8. Setelah Anda selesai menambahkan set kontrol dan kontrol, pilih Berikutnya.

Langkah 3: Tinjau dan buat kerangka kerja

Tinjau informasi untuk kerangka kerja Anda. Untuk mengubah informasi untuk satu langkah, pilih Edit.

Setelah selesai, pilih Buat kerangka kerja khusus.

Langkah selanjutnya

Setelah Anda membuat kerangka kustom baru, Anda dapat membuat penilaian dari kerangka kerja Anda. Untuk informasi selengkapnya, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk meninjau kembali kerangka kerja khusus Anda di kemudian hari, lihat [Menemukan kerangka kerja yang tersedia di AWS Audit Manager](#). Anda dapat mengikuti langkah-langkah ini untuk menemukan kerangka kerja khusus Anda sehingga Anda kemudian dapat melihat, mengedit, berbagi, atau menghapusnya.

Sumber daya tambahan

Untuk solusi untuk masalah kerangka kerja di Audit Manager, lihat [Memecahkan masalah kerangka kerja](#).

Mengedit kerangka kerja khusus di AWS Audit Manager

Anda mungkin perlu memodifikasi kerangka kerja kustom Anda AWS Audit Manager saat persyaratan kepatuhan Anda berubah.

Halaman ini menguraikan langkah-langkah untuk mengedit detail kerangka kerja kustom dan kumpulan kontrol.

Prasyarat

Prosedur berikut mengasumsikan bahwa Anda sebelumnya telah membuat kerangka kerja khusus.

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk mengedit kerangka kerja khusus di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Tugas

- [Langkah 1: Edit detail kerangka kerja](#)
- [Langkah 2: Edit set kontrol](#)
- [Langkah 3. Tinjau dan simpan](#)

Langkah 1: Edit detail kerangka kerja

Mulailah dengan meninjau dan mengedit detail kerangka kerja yang ada.

Untuk mengedit detail kerangka kerja

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi kiri, pilih pustaka Framework dan kemudian pilih tab Kerangka kerja khusus.

3. Pilih kerangka kerja yang ingin Anda edit, pilih Tindakan, lalu pilih Edit.
 - Atau, buka kerangka kerja khusus dan pilih Edit di kanan atas halaman detail kerangka kerja.
4. Di bawah Detail Framework, tinjau nama, jenis kepatuhan, dan deskripsi untuk kerangka kerja Anda, dan buat perubahan yang diperlukan.
5. Pilih Berikutnya.

Tip

Untuk mengedit tag untuk kerangka kerja, buka kerangka kerja dan pilih tab tag [kerangka kerja](#). Di sana Anda dapat melihat dan mengedit tag yang terkait dengan kerangka kerja.

Langkah 2: Edit set kontrol

Selanjutnya, tinjau dan edit kontrol dan kumpulan kontrol dalam kerangka kerja.

Note

Saat Anda menggunakan AWS Audit Manager konsol untuk mengedit kerangka kerja khusus, Anda dapat menambahkan hingga 10 set kontrol untuk setiap kerangka kerja.

Saat Anda menggunakan Audit Manager API untuk mengedit kerangka kerja khusus, Anda dapat menambahkan lebih dari 10 set kontrol. Untuk menambahkan lebih banyak kumpulan kontrol daripada yang diizinkan konsol saat ini, gunakan [UpdateAssessmentFramework](#) API yang disediakan Audit Manager.

Untuk mengedit kumpulan kontrol

1. Di bawah Nama set kontrol, tinjau dan edit nama untuk kumpulan kontrol Anda sesuai kebutuhan.
2. Di bawah Tambahkan kontrol, gunakan daftar tarik-turun Jenis kontrol untuk memilih salah satu dari dua jenis kontrol: Kontrol standar atau Kontrol khusus.
3. Berdasarkan opsi yang Anda pilih pada langkah sebelumnya, daftar tabel kontrol standar atau kontrol khusus ditampilkan. Pilih satu atau lebih kontrol dan pilih Tambahkan ke kumpulan kontrol.

4. Di jendela pop-up yang muncul, pilih **Tambah**.
5. Tinjau dan edit kontrol yang muncul di daftar kontrol yang dipilih.
 - Untuk menambahkan lebih banyak kontrol, ulangi langkah 2—4.
 - Untuk menghapus kontrol yang tidak diinginkan, pilih satu atau beberapa kontrol dan pilih **Hapus** dari kumpulan kontrol.
6. Untuk menambahkan kumpulan kontrol baru ke kerangka kerja, pilih **Tambahkan set kontrol**.
7. Untuk menghapus kumpulan kontrol yang tidak diinginkan, pilih **Hapus kumpulan kontrol**.
8. Setelah Anda selesai menambahkan set kontrol dan kontrol, pilih **Berikutnya**.

Langkah 3. Tinjau dan simpan

Tinjau informasi untuk kerangka kerja Anda. Untuk mengubah informasi untuk satu langkah, pilih **Edit**.

Setelah Anda selesai, pilih **Simpan perubahan**.

Langkah selanjutnya

Ketika Anda yakin bahwa Anda tidak lagi memerlukan kerangka kerja khusus, Anda dapat membersihkan lingkungan Manajer Audit Anda dengan menghapus kerangka kerja. Untuk petunjuk, lihat [Menghapus kerangka kerja khusus di AWS Audit Manager](#).

Sumber daya tambahan

Untuk solusi untuk masalah kerangka kerja di Audit Manager, lihat [Memecahkan masalah kerangka kerja](#).

Berbagi kerangka kerja khusus di AWS Audit Manager

Anda dapat menggunakan fitur berbagi kerangka kerja AWS Audit Manager untuk mereplikasi kerangka kerja khusus yang Anda buat dengan cepat. Anda dapat membagikan kerangka kerja khusus Anda dengan yang lain Akun AWS, atau mereplikasi kerangka kerja Anda ke yang lain Wilayah AWS di bawah akun Anda sendiri. Penerima kemudian dapat mengakses kerangka kerja khusus Anda dan menggunakannya untuk membuat penilaian. Mereka dapat melakukan ini tanpa harus mengulangi upaya konfigurasi Anda untuk kerangka kerja itu.

Poin kunci

Untuk berbagi kerangka kerja khusus, Anda membuat permintaan berbagi. Penerima permintaan berbagi kemudian memiliki 120 hari untuk menerima atau menolak permintaan. Ketika mereka menerima permintaan berbagi, Audit Manager mereplikasi kerangka kerja khusus bersama ke pustaka kerangka kerja mereka. Selain mereplikasi kerangka kerja khusus, Audit Manager juga mereplikasi kumpulan kontrol kustom dan kontrol khusus yang merupakan bagian dari kerangka kerja tersebut. Kontrol kustom ini kemudian ditambahkan ke pustaka kontrol penerima. Audit Manager tidak mereplikasi kerangka kerja atau kontrol standar. Secara default, ini tersedia di semua Akun AWS dan Wilayah di mana Manajer Audit diaktifkan.

Fitur berbagi kerangka kerja hanya tersedia pada tingkat berbayar. Namun, tidak ada biaya tambahan untuk berbagi kerangka kerja khusus atau menerima permintaan berbagi. Untuk mempelajari lebih lanjut tentang penetapan harga AWS Audit Manager, lihat halaman [AWS Audit Manager harga](#).

Important

Anda tidak boleh membagikan kerangka kerja khusus yang berasal dari kerangka standar jika kerangka standar ditetapkan sebagai tidak memenuhi syarat untuk dibagikan oleh AWS, kecuali Anda telah memperoleh izin untuk melakukannya dari pemilik kerangka standar. Untuk melihat kerangka kerja standar mana yang tidak memenuhi syarat untuk dibagikan dan mempelajari lebih lanjut, lihat Kelayakan berbagi [kerangka kerja](#).

Sumber daya tambahan

Untuk mempelajari selengkapnya tentang cara berbagi kerangka kerja khusus di Audit Manager, lihat sumber daya berikut.

- [Kerangka kerja berbagi konsep dan terminologi](#)
- [Mengirim permintaan untuk berbagi kerangka kerja khusus di AWS Audit Manager](#)
- [Menanggapi permintaan berbagi di AWS Audit Manager](#)
- [Menghapus permintaan berbagi di AWS Audit Manager](#)

Kerangka kerja berbagi konsep dan terminologi

Jika Anda mempelajari tentang konsep-konsep kunci berikut, Anda bisa mendapatkan lebih banyak dari fitur berbagi kerangka kerja AWS Audit Manager khusus.

Poin kunci

Sender

Ini adalah pembuat permintaan berbagi dan Akun AWS tempat kerangka kerja khusus ada. Pengirim dapat berbagi kerangka kerja khusus dengan apa pun Akun AWS. Atau, mereka mereplikasi kerangka kerja khusus ke yang didukung Wilayah AWS di bawah akun mereka sendiri.

Penerima

Ini adalah konsumen dari kerangka kerja bersama. Penerima dapat menerima atau menolak permintaan berbagi dari pengirim.

Note

Penerima dapat berupa akun administrator yang didelegasikan. Namun, Anda tidak dapat berbagi kerangka kerja khusus dengan akun AWS Organizations manajemen.

Kelayakan kerangka kerja

Anda hanya dapat berbagi kerangka kerja khusus. Secara default, kerangka kerja standar sudah ada di semua Akun AWS dan Wilayah AWS di mana AWS Audit Manager diaktifkan. Selain itu, kerangka kerja khusus yang Anda bagikan tidak boleh berisi data sensitif. Ini termasuk data yang ditemukan dalam kerangka itu sendiri, kumpulan kontrolnya, dan salah satu kontrol khusus yang merupakan bagian dari kerangka kerja khusus.

Important

Beberapa kerangka kerja standar yang ditawarkan oleh AWS Audit Manager berisi materi berhak cipta yang tunduk pada perjanjian lisensi. Kerangka kerja khusus mungkin berisi konten yang berasal dari kerangka kerja ini. Anda tidak boleh membagikan kerangka kerja khusus yang berasal dari kerangka standar jika kerangka standar ditetapkan sebagai tidak memenuhi syarat untuk dibagikan oleh AWS, kecuali Anda telah memperoleh izin untuk melakukannya dari pemilik kerangka standar.

Untuk mempelajari kerangka kerja standar mana yang memenuhi syarat untuk dibagikan, lihat tabel berikut.

Nama kerangka standar	Versi kustom yang memenuhi syarat untuk dibagikan
Pusat Keamanan Cyber Australia (ACSC) Esensial Delapan	☑Ya
Manual Keamanan Informasi Pusat Keamanan Cyber Australia (ACSC) (ISM) 02 Maret 2023	☑Ya
Kerangka Kerja Contoh Manajer Audit Amazon Web Services (AWS)	☑Ya
AWS Control Tower pagar pembatas	☑Ya
AWS Kerangka Praktik Terbaik AI generatif v2	☑Ya
AWS Manajer Lisensi	☑Ya
AWS Praktik Terbaik Keamanan Dasar	☑Ya
AWS Praktik Terbaik Operasional	☑Ya
Layanan Web Amazon (AWS) Kerangka Kerja Berarsitektur Baik (WAF) v10	☑Ya
Pusat Keamanan Cyber Kanada (CCCS) Kontrol Awan Sedang	☒Tidak
Pusat Keamanan Internet (CIS) Layanan Web Amazon (AWS) Benchmark v1.2.0, Level 1	☒Tidak
Pusat Keamanan Internet (CIS) Layanan Web Amazon (AWS) Benchmark v1.2.0, Level 1 dan 2	☒Tidak
Pusat Keamanan Internet (CIS) Layanan Web Amazon (AWS) Benchmark v1.3.0, Level 1	☒Tidak

Nama kerangka standar	Versi kustom yang memenuhi syarat untuk dibagikan
Pusat Keamanan Internet (CIS) Layanan Web Amazon (AWS) Benchmark v1.3.0, Level 1 dan 2	⊗Tidak
Pusat Keamanan Internet (CIS) Layanan Web Amazon (AWS) Benchmark v1.4.0, Level 1	⊗Tidak
Pusat Keamanan Internet (CIS) Layanan Web Amazon (AWS) Benchmark v1.4.0, Level 1 dan 2	⊗Tidak
Pusat Keamanan Internet (CIS) v7.1, IG1	☑Ya
Kontrol Keamanan Kritis CIS versi 8.0 (CIS v8.0), IG1	⊗Tidak
Program Manajemen Risiko Dan Otorisasi Federal (FedRAMP) Kontrol Dasar Keamanan r4, Sedang	☑Ya
Peraturan Perlindungan Data Umum (GDPR) 2016	☑Ya
Gramm-Leach-Bliley Tindakan (GLBA)	☑Ya
Judul 21 Kode Peraturan Federal (CFR) Bagian 11, Catatan elektronik; Tanda Tangan Elektronik - Ruang Lingkup dan Aplikasi 24 Mei 2023	☑Ya
EudraLex - Aturan yang Mengatur Produk Obat di Uni Eropa (UE) - Volume 4: Good Manufacturing Practice (GMP) Produk Obat untuk Penggunaan Manusia dan Hewan - Lampiran 11	☑Ya
Aturan Keamanan Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA): Februari 2003	☑Ya
Aturan Akhir Omnibus Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA)	☑Ya

Nama kerangka standar	Versi kustom yang memenuhi syarat untuk dibagikan
Organisasi Internasional untuk Standardisasi (ISO) /Komisi Elektroteknik Internasional (IEC) 27001:2013 Lampiran A	⊗Tidak
NIST 800-53 Rev 5: Kontrol Keamanan dan Privasi untuk Sistem Informasi dan Organisasi	✔Ya
Kerangka Kerja Keamanan Siber NIST (CSF) v1.1	✔Ya
NIST 800-171 Revisi 2: Melindungi Informasi Tak Terklasifikasi yang Terkendali dalam Sistem dan Organisasi Nonfederal	✔Ya
Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) v3.2.1	⊗Tidak
Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) v4.0	⊗Tidak
Pernyataan tentang Standar untuk Keterlibatan Pengesahan (SSAE) No. 18, Laporan Kontrol Organisasi Layanan (SOC) 2	⊗Tidak

Bagikan permintaan

Untuk berbagi kerangka kerja khusus, Anda membuat permintaan berbagi. Permintaan berbagi menentukan penerima dan memberi tahu mereka bahwa kerangka kerja khusus tersedia. Penerima memiliki waktu 120 hari untuk menanggapi permintaan berbagi dengan menerima atau menolak. Jika tidak ada tindakan yang diambil dalam 120 hari, permintaan berbagi kedaluwarsa dan penerima kehilangan kemampuan untuk menambahkan kerangka kerja khusus ke pustaka kerangka kerja mereka. Pengirim dan penerima dapat melihat dan mengambil tindakan pada permintaan berbagi dari halaman permintaan berbagi pustaka kerangka kerja.

Status permintaan berbagi

Permintaan berbagi dapat memiliki salah satu status berikut.

Status	Deskripsi
Aktif	Ini menunjukkan permintaan berbagi yang berhasil dikirim ke penerima dan sedang menunggu tanggapan mereka.
Kedaluwarsa	Ini menunjukkan permintaan berbagi yang kedaluwarsa dalam 30 hari ke depan.
Berbagi	Ini menunjukkan permintaan berbagi yang diterima penerima.
Tidak aktif	Ini menunjukkan permintaan berbagi yang dicabut, ditolak, atau kedaluwarsa sebelum penerima mengambil tindakan.
Mereplikasi	Ini menunjukkan permintaan berbagi yang diterima yang sedang direplikasi ke pustaka kerangka penerima.
Gagal	Ini menunjukkan permintaan berbagi yang tidak berhasil dikirim ke penerima.

Bagikan pemberitahuan permintaan

Audit Manager memberi tahu penerima saat mereka menerima permintaan berbagi. Penerima dan pengirim menerima pemberitahuan ketika permintaan berbagi akan kedaluwarsa dalam 30 hari ke depan.

- Untuk penerima, titik pemberitahuan biru muncul di sebelah permintaan yang diterima dengan status **Aktif** atau **Kedaluwarsa**. Penerima dapat menyelesaikan notifikasi dengan menerima atau menolak permintaan berbagi.
- Untuk pengirim, titik pemberitahuan biru muncul di sebelah permintaan terkirim dengan status **Kedaluwarsa**. Pemberitahuan diselesaikan ketika penerima menerima atau menolak permintaan. Jika tidak, itu diselesaikan ketika permintaan kedaluwarsa. Selain itu, pengirim dapat menyelesaikan notifikasi dengan mencabut permintaan berbagi.

Kepemilikan pengirim

Pengirim mempertahankan akses penuh atas kerangka kerja khusus yang mereka bagikan. Mereka dapat membatalkan permintaan berbagi aktif kapan saja dengan [mencabut permintaan berbagi](#) sebelum kedaluwarsa. Namun, setelah penerima menerima permintaan berbagi, pengirim tidak dapat lagi mencabut akses penerima ke kerangka kerja khusus tersebut. Ini

karena ketika penerima menerima permintaan, Audit Manager membuat salinan independen dari kerangka kerja khusus di pustaka kerangka kerja penerima.

Selain mereplikasi kerangka kerja khusus pengirim, Audit Manager juga mereplikasi kumpulan kontrol kustom dan kontrol khusus yang merupakan bagian dari kerangka kerja tersebut. Namun, Audit Manager tidak mereplikasi tag apa pun yang dilampirkan ke kerangka kerja khusus.

Kepemilikan penerima

Penerima memiliki akses penuh atas kerangka kerja khusus yang mereka terima. Saat penerima menerima permintaan, Audit Manager mereplikasi kerangka kerja khusus ke tab kerangka kerja khusus dari pustaka kerangka kerja mereka. Penerima kemudian dapat mengelola kerangka kerja kustom bersama dengan cara yang sama seperti kerangka kerja khusus lainnya. Penerima dapat berbagi kerangka kerja khusus yang mereka terima dari pengirim lain. Penerima tidak dapat memblokir pengirim agar tidak mengirim permintaan berbagi.

Kedaluwarsa kerangka kerja bersama

Saat pengirim membuat permintaan berbagi, Audit Manager menetapkan permintaan untuk kedaluwarsa setelah 120 hari. Penerima dapat menerima dan mendapatkan akses ke kerangka kerja bersama sebelum permintaan berakhir. Jika penerima tidak menerima selama waktu ini, permintaan berbagi kedaluwarsa. Setelah titik ini, catatan permintaan saham yang kedaluwarsa tetap ada dalam sejarah mereka. Snapshot kerangka kerja bersama yang kedaluwarsa diarsipkan ke bucket S3 dengan TTL satu tahun untuk tujuan audit.

Pengirim dapat memilih [untuk mencabut permintaan berbagi](#) kapan saja sebelum kedaluwarsa.

Penyimpanan dan pencadangan data kerangka kerja bersama

Saat Anda membuat permintaan berbagi, Audit Manager menyimpan snapshot kerangka kerja kustom Anda di AS Timur (Virginia Utara) Wilayah AWS. Audit Manager juga menyimpan cadangan dari snapshot yang sama di AS Barat (Oregon) Wilayah AWS.

Audit Manager menghapus snapshot dan snapshot cadangan ketika salah satu peristiwa berikut terjadi:

- Pengirim mencabut permintaan berbagi.
- Penerima menolak permintaan berbagi.
- Penerima mengalami kesalahan dan tidak berhasil menerima permintaan berbagi.
- Permintaan berbagi kedaluwarsa sebelum penerima menanggapi permintaan tersebut.

Saat pengi [rim mengirim ulang permintaan berbagi](#), snapshot diganti dengan versi terbaru yang sesuai dengan versi terbaru kerangka kerja khusus.

Ketika penerima menerima permintaan berbagi, snapshot direplikasi ke dalam permintaan berbagi Akun AWS di bawah Wilayah AWS yang ditentukan dalam permintaan berbagi.

Versi kerangka kerja bersama

Saat Anda berbagi kerangka kerja khusus, Manajer Audit membuat salinan independen dari kerangka kerja tersebut di Wilayah Akun AWS dan yang ditentukan. Ini berarti bahwa Anda harus mengingat poin-poin berikut:

- Kerangka kerja bersama yang diterima penerima adalah snapshot dari kerangka kerja pada saat pembuatan permintaan berbagi. Jika Anda memperbarui kerangka kerja khusus asli setelah mengirim permintaan berbagi, permintaan tidak diperbarui secara otomatis. Untuk membagikan versi terbaru dari kerangka kerja yang diperbarui, Anda dapat [mengirim ulang permintaan](#) berbagi. Tanggal kedaluwarsa snapshot baru ini adalah 120 hari sejak tanggal pembagian ulang.
- Saat Anda berbagi kerangka kerja khusus dengan yang lain Akun AWS dan kemudian menghapusnya dari pustaka kerangka kerja Anda, kerangka kerja kustom bersama tetap berada di pustaka kerangka kerja penerima.
- Saat Anda membagikan kerangka kerja khusus ke yang lain Wilayah AWS di bawah akun Anda dan kemudian menghapus kerangka kerja khusus itu di yang pertama Wilayah AWS, kerangka kerja kustom tetap berada di Wilayah kedua.
- Saat Anda menghapus kerangka kerja kustom bersama setelah menerimanya, kontrol kustom apa pun yang direplikasi sebagai bagian dari kerangka kerja kustom tetap ada di pustaka kontrol Anda.

Sumber daya tambahan

- [Mengirim permintaan untuk berbagi kerangka kerja khusus di AWS Audit Manager](#)
- [Menanggapi permintaan berbagi di AWS Audit Manager](#)
- [Menghapus permintaan berbagi di AWS Audit Manager](#)
- [Memecahkan masalah kerangka kerja](#)

Mengirim permintaan untuk berbagi kerangka kerja khusus di AWS Audit Manager

Tutorial ini menjelaskan cara berbagi kerangka kerja khusus Anda di seluruh Akun AWS dan Wilayah AWS.

Saat Anda berbagi kerangka kerja khusus, Audit Manager membuat snapshot kerangka kerja Anda dan mengirimkan permintaan berbagi ke penerima. Penerima memiliki waktu 120 hari untuk menerima kerangka kerja bersama. Ketika mereka menerima, Audit Manager mereplikasi kerangka kerja khusus bersama ke pustaka kerangka kerja mereka dalam yang ditentukan Wilayah AWS. Jika Anda ingin mereplikasi kerangka kerja khusus ke Wilayah lain di bawah akun Anda sendiri, gunakan tutorial berikut dan masukkan Akun AWS ID Anda sendiri sebagai ID akun penerima.

Prasyarat

Sebelum Anda memulai tutorial ini, pastikan bahwa Anda terlebih dahulu memenuhi persyaratan berikut:

- Anda akrab dengan [kerangka kerja Audit Manager berbagi konsep dan terminologi](#).
- Kerangka kerja khusus yang ingin Anda bagikan [memenuhi syarat untuk dibagikan](#) dan ada di pustaka kerangka kerja AWS Audit Manager lingkungan Anda.
- Penerima sudah diaktifkan AWS Audit Manager di Wilayah AWS tempat Anda ingin berbagi kerangka kerja khusus.
- Penerima bukan akun AWS Organizations manajemen.
- Identitas IAM Anda memiliki izin yang sesuai untuk berbagi kerangka kerja khusus di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Tip

Sebelum memulai, catat Akun AWS ID yang ingin Anda bagikan kerangka kustom Anda. Ini bisa menjadi ID akun Anda sendiri, jika tujuan Anda adalah mereplikasi kerangka kerja ke yang lain Wilayah AWS di bawah akun Anda. Anda memerlukan informasi ini untuk langkah 2 dari tutorial.

Prosedur

Tugas

- [Langkah 1: Identifikasi kerangka kerja khusus yang ingin Anda bagikan](#)
- [Langkah 2: Kirim permintaan berbagi](#)
- [Langkah 3: Lihat permintaan yang Anda kirim](#)
- [Langkah 4 \(Opsional\): Cabut permintaan berbagi](#)

Langkah 1: Identifikasi kerangka kerja khusus yang ingin Anda bagikan

Mulailah dengan mengidentifikasi kerangka kerja khusus yang ingin Anda bagikan. Anda dapat menemukan daftar semua kerangka kerja khusus yang tersedia di halaman pustaka Framework di Audit Manager.

Important

Jangan berbagi kerangka kerja khusus yang berisi data sensitif. Ini termasuk data yang ditemukan dalam kerangka itu sendiri, kumpulan kontrolnya, dan salah satu kontrol khusus yang terdiri dari kerangka kerja khusus. Untuk informasi selengkapnya, lihat [Kelayakan Framework](#).

Untuk melihat kerangka kerja khusus yang tersedia

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi, pilih pustaka Framework.
3. Pilih tab Kerangka kerja khusus. Ini menampilkan daftar kerangka kerja khusus yang tersedia. Anda dapat memilih nama kerangka kerja apa pun untuk melihat detail kerangka kerja khusus itu.

Langkah 2: Kirim permintaan berbagi

Selanjutnya, tentukan penerima dan kirimkan permintaan berbagi untuk kerangka kerja khusus. Penerima memiliki 120 hari untuk menanggapi permintaan berbagi sebelum kedaluwarsa.

Untuk mengirim permintaan berbagi

1. Dari tab Kerangka kerja khusus pada pustaka kerangka kerja, pilih nama kerangka kerja untuk membuka halaman detail. Dari sini, pilih Tindakan dan kemudian pilih Bagikan kerangka kerja khusus.
 - Atau, pilih kerangka kerja khusus dari daftar di pustaka kerangka kerja, pilih Tindakan, lalu pilih Bagikan kerangka kerja khusus. Tergantung pada ukuran kerangka kerja khusus, metode ini dapat memakan waktu beberapa detik sementara Audit Manager menyiapkan permintaan berbagi.
2. Tinjau pemberitahuan yang ditampilkan di kotak dialog.
 - Jika Anda tidak yakin apakah Anda dapat membagikan kerangka kerja khusus Anda, tinjau kelayakan [Framework](#) untuk panduan lebih lanjut.
 - Jika kerangka kerja Anda memiliki kontrol yang menggunakan AWS Config aturan khusus sebagai sumber data, sebaiknya hubungi penerima untuk memberi tahu mereka. Penerima kemudian dapat membuat dan mengaktifkan AWS Config aturan yang sama dalam instance mereka AWS Config. Untuk informasi selengkapnya, lihat [Kerangka kerja bersama saya memiliki kontrol yang menggunakan kustom AWS Config aturan sebagai sumber data. Dapatkah penerima mengumpulkan bukti untuk kontrol ini?](#).
3. Mas **agree** uk dan kemudian pilih Setuju untuk melanjutkan.
4. Pada layar berikutnya, ikuti langkah-langkah ini:
 - Di bawah Akun AWS, masukkan ID akun penerima. Ini bisa menjadi ID akun Anda sendiri.
 - Di bawah Wilayah AWS, pilih Wilayah penerima dari daftar dropdown.
 - (Opsional) Di bawah Pesan ke penerima, masukkan komentar opsional tentang kerangka kerja khusus yang Anda bagikan.
 - Di bawah Detail kerangka kerja khusus, tinjau detailnya untuk mengonfirmasi bahwa Anda ingin membagikan kerangka kerja ini.
5. Pilih Bagikan.

Note

Ingatlah poin-poin berikut:

- Ketika Anda berbagi kerangka kerja khusus dengan yang lain Akun AWS, kerangka kerja direplikasi hanya ke yang ditentukan Wilayah AWS. Setelah menerima permintaan

berbagi, penerima kemudian dapat mereplikasi kerangka kerja di seluruh Wilayah sesuai kebutuhan.

- Saat berbagi kerangka kerja khusus Wilayah AWS, diperlukan waktu hingga 10 menit untuk memproses tindakan permintaan berbagi. Setelah mengirim permintaan berbagi lintas wilayah, sebaiknya periksa kembali nanti untuk mengonfirmasi bahwa permintaan berbagi berhasil dikirim.
- Saat Anda mengirim permintaan berbagi, Audit Manager mengambil snapshot dari kerangka kerja khusus pada saat pembuatan permintaan berbagi. Jika Anda memperbarui kerangka kerja khusus setelah mengirim permintaan berbagi, permintaan tidak diperbarui secara otomatis. Untuk membagikan versi terbaru dari kerangka kerja yang diperbarui, Anda dapat [mengirim ulang permintaan](#) berbagi. Tanggal kedaluwarsa snapshot baru ini adalah 120 hari sejak tanggal pembagian ulang.

Langkah 3: Lihat permintaan yang Anda kirim

Anda dapat memilih tab **Permintaan terkirim** untuk melihat daftar semua permintaan berbagi yang Anda kirim. Anda dapat memfilter daftar ini sesuai kebutuhan. Misalnya, Anda dapat menerapkan filter untuk hanya menampilkan permintaan yang kedaluwarsa dalam 30 hari ke depan.

Untuk melihat dan memfilter permintaan yang dikirim

1. Dari panel navigasi, pilih **Bagikan permintaan**.
2. Pilih tab **Permintaan Terkirim**.
3. (Opsional) Terapkan filter untuk menyempurnakan permintaan terkirim mana yang terlihat. Anda dapat melakukan ini dengan menemukan daftar dropdown **Semua status**, dan mengubah filter ke salah satu dari berikut ini.

Status	Deskripsi
Aktif	Filter ini menampilkan permintaan berbagi yang sedang menunggu tanggapan dari penerima.
Kedaluwarsa	Filter ini menampilkan permintaan berbagi yang kedaluwarsa dalam 30 hari ke depan.

Status	Deskripsi
Berbagi	Filter ini menampilkan permintaan berbagi yang diterima oleh penerima. Kerangka kerja kustom bersama sekarang ada di pustaka kerangka kerja penerima.
Tidak aktif	Filter ini menampilkan permintaan berbagi yang ditolak, dicabut, atau kedaluwarsa sebelum penerima mengambil tindakan. Pilih kata Tidak aktif untuk melihat detail lebih lanjut.
Mereplikasi	Ini menunjukkan permintaan berbagi yang diterima yang sedang direplikasi ke pustaka kerangka penerima.
Gagal	Filter ini menampilkan permintaan berbagi yang tidak berhasil dikirim ke penerima. Pilih kata Gagal untuk melihat detail selengkapnya.

Note

Diperlukan waktu hingga 15 menit untuk memproses permintaan berbagi. Akibatnya, jika terjadi kesalahan saat mengirim permintaan berbagi ke penerima, status Gagal mungkin tidak segera ditampilkan. Sebaiknya periksa kembali nanti untuk mengonfirmasi bahwa permintaan berbagi berhasil dikirim.

Langkah 4 (Opsional): Cabut permintaan berbagi

Jika Anda perlu membatalkan permintaan berbagi aktif sebelum kedaluwarsa, Anda dapat mencabut permintaan kapan saja. Langkah ini bersifat opsional. Jika Anda tidak mengambil tindakan, penerima kehilangan kemampuan untuk menerima permintaan berbagi setelah tanggal kedaluwarsa.

Untuk mencabut permintaan berbagi

1. Dari panel navigasi, pilih **Bagikan permintaan**.
2. Pilih tab **Permintaan Terkirim**.
3. Pilih kerangka kerja yang ingin Anda cabut dan pilih **Cabut permintaan**.
4. Di jendela pop-up yang muncul, pilih **Cabut**.

 Note

Anda hanya dapat mencabut akses ke permintaan berbagi yang memiliki status **Aktif** atau **Kedaluwarsa**. Setelah penerima menerima permintaan berbagi, Anda tidak dapat lagi mencabut aksesnya ke kerangka kerja khusus tersebut. Ini karena salinan kerangka kerja khusus sekarang ada di pustaka kerangka penerima.

Saat berbagi kerangka kerja Wilayah AWS, diperlukan waktu hingga 10 menit untuk memproses tindakan permintaan berbagi. Setelah mencabut permintaan berbagi lintas wilayah, sebaiknya periksa kembali nanti untuk mengonfirmasi bahwa permintaan berbagi berhasil dicabut.

Langkah selanjutnya

Mengirim ulang permintaan berbagi untuk kerangka kerja yang diperbarui

Anda dapat mengirim permintaan berbagi untuk kerangka kerja khusus dan kemudian memperbarui kerangka kerja yang sama setelahnya. Jika Anda melakukan ini, permintaan berbagi tidak diperbarui secara otomatis untuk mencerminkan versi terbaru kerangka kerja. Namun, jika statusnya **aktif**, **di bagikan**, atau **kedaluwarsa**, Anda dapat memperbarui permintaan berbagi yang ada. Untuk melakukan ini, Anda mengirim ulang permintaan berbagi baru dengan kumpulan detail yang sama dengan permintaan yang ada. Dalam permintaan berbagi baru, sertakan ID kerangka kerja khusus, ID akun penerima, dan penerima yang sama Wilayah AWS. Anda juga dapat memberikan komentar baru dengan permintaan berbagi baru.

Ingatlah hal-hal berikut saat Anda mengirim ulang permintaan berbagi:

- Agar pembaruan berhasil, permintaan baru harus untuk ID kerangka kerja kustom yang sama. Itu juga harus menentukan ID akun penerima dan Wilayah yang sama dengan permintaan yang ada.
- Jika nama kerangka kustom telah berubah, permintaan berbagi yang diperbarui menampilkan nama terbaru.
- Jika Anda memberikan komentar baru, permintaan berbagi yang diperbarui menampilkan komentar terbaru.
- Saat Anda mengirim ulang permintaan berbagi, tanggal kedaluwarsa diperpanjang enam bulan.

Untuk mengirim ulang permintaan berbagi untuk kerangka kerja yang diperbarui

1. Dari tab Kerangka kerja khusus pada pustaka kerangka kerja, pilih nama kerangka kerja yang ingin Anda bagikan. Ini membuka halaman detail kerangka kerja.
2. Pilih Tindakan dan kemudian pilih Bagikan kerangka kerja khusus.
3. Tinjau pemberitahuan yang ditampilkan di kotak dialog, masukkan **agree**, lalu pilih Setuju untuk melanjutkan.
4. Pada layar berikutnya, ikuti langkah-langkah ini:
 - Di bawah Akun AWS, masukkan ID akun yang sama yang Anda tentukan dalam permintaan berbagi yang ada.
 - Di bawah Wilayah AWS, pilih Wilayah yang sama yang Anda tentukan dalam permintaan berbagi yang ada.
 - (Opsional) Di bawah Pesan ke penerima, masukkan komentar opsional tentang kerangka kerja kustom yang diperbarui.
 - Di bawah Detail kerangka kerja khusus, tinjau detail untuk mengonfirmasi bahwa Anda ingin mengirim ulang permintaan berbagi.
5. Pilih Bagikan untuk mengirim ulang dan memperbarui permintaan berbagi.

Sumber daya tambahan

Untuk menemukan solusi untuk masalah yang mungkin Anda temui saat berbagi kerangka kerja khusus, lihat [Memecahkan masalah kerangka kerja](#).

Menanggapi permintaan berbagi di AWS Audit Manager

Tutorial ini menjelaskan tindakan yang harus diambil ketika Anda menerima permintaan berbagi untuk kerangka kerja khusus. Manajer Audit memberi tahu Anda ketika Anda menerima permintaan berbagi. Anda juga menerima pemberitahuan untuk mengingatkan Anda ketika permintaan berbagi akan kedaluwarsa dalam 30 hari ke depan.

Prasyarat

Sebelum memulai, sebaiknya Anda terlebih dahulu mempelajari lebih lanjut tentang konsep dan terminologi berbagi [kerangka kerja Audit Manager](#).

Prosedur

Tugas

- [Langkah 1: Periksa pemberitahuan permintaan yang Anda terima](#)
- [Langkah 2: Ambil tindakan atas permintaan](#)
- [Langkah 3: Lihat riwayat permintaan yang Anda terima](#)

Langkah 1: Periksa pemberitahuan permintaan yang Anda terima

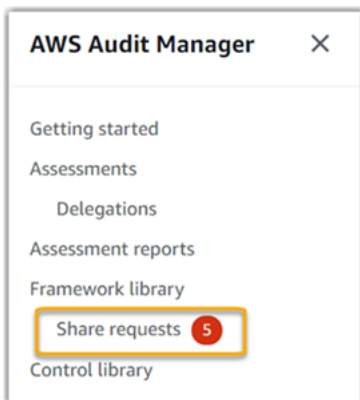
Mulailah dengan memeriksa notifikasi permintaan berbagi Anda. Tab **Permintaan yang diterima** menampilkan daftar permintaan berbagi yang telah Anda terima dari orang lain Akun AWS. Permintaan yang menunggu tanggapan Anda muncul dengan titik biru. Anda juga dapat memfilter tampilan ini untuk hanya menampilkan permintaan yang kedaluwarsa dalam waktu 30 hari ke depan.

Untuk melihat permintaan yang diterima

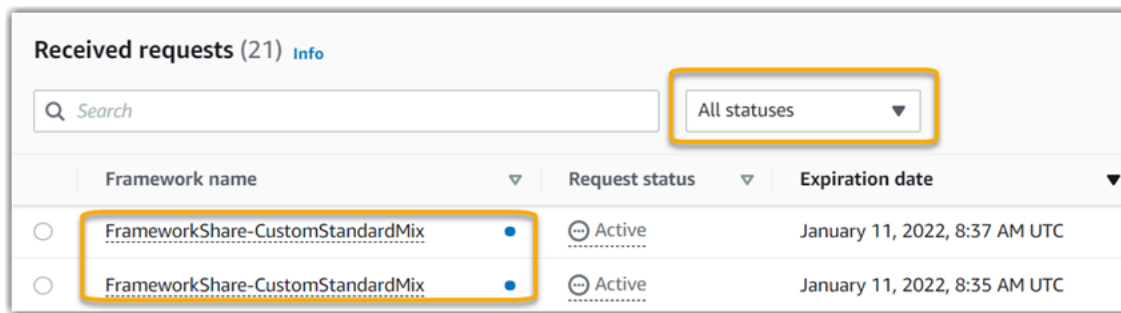
1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Jika Anda memiliki pemberitahuan permintaan berbagi, Audit Manager menampilkan titik merah di sebelah ikon menu navigasi.



3. Perluas panel navigasi dan lihat di sebelah **Bagikan permintaan**. Lencana notifikasi menunjukkan jumlah permintaan berbagi yang perlu Anda perhatikan.



4. Pilih **Bagikan permintaan**. Secara default, halaman ini terbuka di tab **Permintaan yang diterima**.
5. Identifikasi permintaan berbagi yang memerlukan tindakan Anda dengan mencari item dengan titik biru.



- (Opsional) Untuk melihat hanya permintaan yang kedaluwarsa dalam 30 hari ke depan, cari daftar dropdown Semua status dan pilih Kedaluwarsa.

Langkah 2: Ambil tindakan atas permintaan

Untuk menghapus titik pemberitahuan biru, Anda perlu mengambil tindakan dengan menerima atau menolak permintaan berbagi.

Menerima kerangka kerja bersama

Saat Anda menerima permintaan berbagi, Audit Manager mereplikasi snapshot dari kerangka kerja asli ke tab kerangka kerja khusus pustaka kerangka kerja Anda. Audit Manager mereplikasi dan mengenkripsi kerangka kerja khusus baru menggunakan kunci KMS yang Anda tentukan di setelan [Audit Manager](#).

Untuk menerima permintaan berbagi

- Buka halaman Permintaan Bagikan dan pastikan Anda melihat tab Per mintaan yang diterima.
- (Opsional) Pilih Aktif atau Kedalu warsa dari daftar tarik-turun filter.
- (Opsional) Pilih nama kerangka kerja untuk melihat detail permintaan berbagi. Ini termasuk informasi seperti deskripsi kerangka kerja, jumlah kontrol yang ada dalam kerangka kerja, dan pesan dari pengirim.
- Pilih permintaan berbagi yang ingin Anda terima, pilih T ind akan, lalu pilih Terima.

Setelah Anda menerima permintaan berbagi, status berubah menjadi mer eplikasi sementara kerangka kerja kustom bersama ditambahkan ke pustaka kerangka kerja Anda. Jika kerangka kerja berisi kontrol khusus, kontrol ini ditambahkan ke pustaka kontrol Anda saat ini.

Ketika replikasi kerangka kerja selesai, status berubah menjadi bersama. Spanduk sukses memberi tahu Anda bahwa kerangka kerja khusus siap digunakan.

 Tip

Ketika Anda menerima kerangka kerja khusus, itu hanya direplikasi ke saat ini Wilayah AWS. Anda mungkin ingin kerangka kerja bersama baru tersedia di semua Wilayah di Akun AWS. Jika demikian, setelah Anda menerima permintaan berbagi, Anda dapat [membagikan kerangka kerja](#) ke Wilayah lain di bawah akun Anda sesuai kebutuhan.

Menolak kerangka kerja bersama

Saat Anda menolak permintaan berbagi, Audit Manager tidak menambahkan kerangka kerja khusus tersebut ke pustaka kerangka kerja Anda. Namun, catatan permintaan berbagi yang ditolak tetap ada di tab **Permintaan yang diterima**, dengan status **Tidak Aktif**.

Menolak permintaan berbagi

1. Buka halaman **Permintaan Bagikan** dan pastikan Anda melihat tab **Permintaan yang diterima**.
2. (Opsional) Pilih **Aktif** atau **Kedaluwarsa** dari daftar tarik-turun filter.
3. (Opsional) Pilih nama kerangka kerja untuk melihat detail permintaan berbagi. Ini termasuk informasi seperti deskripsi kerangka kerja, jumlah kontrol yang ada dalam kerangka kerja, dan pesan dari pengirim.
4. Pilih permintaan berbagi yang ingin Anda tolak, pilih **Tindakan**, lalu pilih **Tolak**.
5. Di kotak dialog yang muncul, pilih **Tolak** untuk mengonfirmasi pilihan Anda.

 Tip

Jika Anda berubah pikiran dan menginginkan akses ke kerangka kerja bersama setelah Anda menolak, minta pengirim untuk mengirimi Anda permintaan berbagi baru.

 Note

Diperlukan waktu hingga 10 menit untuk memproses tindakan permintaan berbagi ketika kerangka kerja dibagikan Wilayah AWS. Setelah mengambil tindakan atas permintaan berbagi lintas wilayah, sebaiknya periksa kembali nanti untuk mengonfirmasi bahwa permintaan berbagi berhasil diterima atau ditolak.

Langkah 3: Lihat riwayat permintaan yang Anda terima

Setelah menerima atau menolak kerangka kerja bersama, Anda dapat kembali ke halaman Permintaan Bagikan untuk melihat riwayat permintaan berbagi. Anda dapat memfilter daftar ini sesuai kebutuhan. Misalnya, Anda dapat menerapkan filter untuk hanya menampilkan permintaan yang Anda terima.

Untuk melihat riwayat permintaan berbagi Anda

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi kiri, pilih **Bagikan permintaan**.
3. Pilih tab **Permintaan yang diterima**.
4. Temukan daftar dropdown **Semua status**, dan pilih salah satu filter berikut:

Nama	Deskripsi
Aktif	Filter ini menampilkan permintaan berbagi yang belum Anda terima atau ditolak.
Kedaluwarsa	Filter ini menampilkan permintaan berbagi yang kedaluwarsa dalam 30 hari ke depan.
Berbagi	Filter ini menampilkan permintaan berbagi yang Anda terima. Kerangka kerja bersama sekarang tersedia di perpustakaan kerangka kerja Anda.
Tidak aktif	Filter ini menampilkan permintaan berbagi yang ditolak atau kedaluwarsa.
Gagal	Filter ini menampilkan permintaan berbagi yang tidak berhasil dikirim. Pilih kata Gagal untuk melihat detail lebih lanjut.

Langkah selanjutnya

Setelah Anda menerima kerangka kerja khusus bersama, Anda dapat menemukannya di tab kerangka kerja khusus dari pustaka kerangka kerja. Anda sekarang dapat menggunakan kerangka kerja itu untuk membuat penilaian. Untuk mempelajari selengkapnya, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk petunjuk tentang cara mengedit kerangka kustom baru Anda, lihat [Mengedit kerangka kerja khusus di AWS Audit Manager](#).

Sumber daya tambahan

Untuk menemukan solusi untuk masalah yang mungkin Anda temui, lihat [Memecahkan masalah kerangka kerja](#).

Menghapus permintaan berbagi di AWS Audit Manager

Jika Anda tidak lagi memerlukan permintaan berbagi, Anda dapat menghapusnya dari lingkungan Manajer Audit Anda. Ini memungkinkan Anda untuk membersihkan ruang kerja Anda dan fokus pada permintaan yang relevan dengan tugas dan prioritas Anda saat ini.

Saat Anda menghapus permintaan berbagi, hanya permintaan itu sendiri yang dihapus. Kerangka kerja bersama itu sendiri tetap ada di perpustakaan kerangka kerja Anda.

Prasyarat

Prosedur berikut mengasumsikan bahwa Anda sebelumnya telah mengirim atau menerima permintaan berbagi. Anda tidak dapat menghapus permintaan berbagi yang memiliki status aktif atau mer epikasi.

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk menghapus permintaan berbagi di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Untuk menghapus permintaan berbagi

1. Dari panel navigasi, pilih Bagikan permintaan.
2. Pilih tab Permintaan Terkirim atau Permintaan yang diterima.
3. Pilih kerangka kerja yang tidak lagi Anda inginkan dan pilih Hapus.
4. Di jendela pop-up yang muncul, pilih Hapus.

Sumber daya tambahan

Untuk menemukan solusi untuk masalah yang mungkin Anda temui, lihat [Memecahkan masalah kerangka kerja](#).

Menghapus kerangka kerja khusus di AWS Audit Manager

Ketika Anda tidak lagi memerlukan kerangka kerja khusus, Anda dapat menghapusnya dari lingkungan Manajer Audit Anda. Ini memungkinkan Anda untuk membersihkan ruang kerja Anda dan fokus pada kerangka kerja khusus yang relevan dengan tugas dan prioritas Anda saat ini.

Prasyarat

Prosedur berikut mengasumsikan bahwa Anda sebelumnya telah membuat kerangka kerja khusus.

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk menghapus kerangka kerja khusus di AWS Audit Manager. Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Anda dapat menghapus kerangka kerja khusus menggunakan konsol Audit Manager, API Manajer Audit, atau AWS Command Line Interface (AWS CLI).

Note

Menghapus kerangka kerja khusus tidak memengaruhi penilaian yang ada yang dibuat dari kerangka kerja sebelum dihapus.

Audit Manager console

Untuk menghapus kerangka kerja khusus di konsol Audit Manager

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi kiri, pilih pustaka Framework dan kemudian pilih tab Kerangka kerja khusus.

3. Pilih kerangka kerja yang ingin Anda hapus, pilih Tindakan, lalu pilih Hapus.
 - Atau, Anda dapat membuka kerangka kerja khusus dan memilih Tindakan, Hapus di kanan atas halaman ringkasan kerangka kerja.
4. Di jendela pop-up, pilih Hapus untuk mengonfirmasi penghapusan.

AWS CLI

Untuk menghapus kerangka kerja khusus di AWS CLI

1. Pertama, identifikasi kerangka kerja khusus yang ingin Anda hapus. Untuk melakukan ini, jalankan [perintah](#) `list-assessment-framework` dan tentukan `--framework-type Custom`

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

Respons mengembalikan daftar kerangka kerja khusus. Temukan kerangka kerja khusus yang ingin Anda hapus, dan catat ID kerangka kerja.

2. Selanjutnya, jalankan [perintah](#) `delete-assessment-framework` dan tentukan kerangka kerja `--framework-id` yang ingin Anda hapus.

Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri.

```
aws auditmanager delete-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

Untuk menghapus kerangka kerja khusus menggunakan API

1. Gunakan [ListAssessmentFrameworks](#) operasi dan tentukan [FrameworkType](#) sebagai `Custom`. Dari tanggapan, temukan kerangka kerja khusus yang ingin Anda hapus, dan catat ID kerangka kerja.
2. Gunakan [DeleteAssessmentFramework](#) operasi untuk menghapus kerangka kerja. Dalam permintaan, gunakan [parameter](#) `frameworkID` untuk menentukan kerangka kerja yang ingin Anda hapus.

Untuk informasi selengkapnya tentang operasi API ini, pilih salah satu tautan di prosedur sebelumnya untuk membaca lebih lanjut di Refer AWS Audit Manager ensi API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasa AWS .

Sumber daya tambahan

Untuk informasi tentang retensi data di Audit Manager, lihat [Penghapusan data Audit Manager](#).

Menggunakan pustaka kontrol untuk mengelola kontrol di AWS Audit Manager

Anda dapat mengakses dan mengelola kontrol dari pustaka kontrol di AWS Audit Manager.

Poin kunci

Di pustaka kontrol, kontrol diatur ke dalam kategori berikut.

- Kontrol umum mengumpulkan bukti yang mendukung beberapa standar kepatuhan yang tumpang tindih. Kontrol umum otomatis berisi satu atau lebih [kontrol inti](#) terkait yang masing-masing mengumpulkan bukti pendukung dari kelompok sumber data yang telah ditentukan sebelumnya. Ini memberi Anda cara yang efisien untuk mengidentifikasi sumber AWS data yang memetakan portofolio persyaratan kepatuhan Anda. Sumber data yang mendasari untuk setiap kontrol umum otomatis divalidasi dan dikelola oleh penilai bersertifikat industri di Layanan [AWS Jaminan Keamanan](#).
- Kontrol standar mengumpulkan bukti untuk mendukung standar kepatuhan tertentu. Anda dapat melihat detail kontrol standar, tetapi Anda tidak dapat mengedit atau menghapusnya. Namun, Anda dapat membuat salinan kontrol standar apa pun yang dapat diedit untuk membuat kontrol baru yang memenuhi persyaratan spesifik Anda.
- Kontrol khusus adalah kontrol yang Anda miliki dan tentukan. Saat Anda membuat kontrol khusus, kami menyarankan Anda memilih kontrol umum yang mewakili tujuan Anda dan menggunakannya sebagai sumber bukti. Akibatnya, kontrol kustom Anda dapat mengumpulkan semua bukti yang relevan dengan kontrol umum tersebut. Anda juga dapat menggunakan kontrol inti sebagai sumber bukti, atau menggunakan sumber lain yang Anda definisikan sendiri. Setelah selesai, tambahkan kontrol kustom Anda ke kerangka kerja kustom, lalu buat penilaian untuk mulai mengumpulkan bukti.

Sumber daya tambahan

Untuk membuat dan mengelola kontrol di Audit Manager, ikuti prosedur yang diuraikan di sini.

- [Menemukan kontrol yang tersedia di AWS Audit Manager](#)
- [Meninjau kontrol di AWS Audit Manager](#)

- [Meninjau kontrol umum](#)
- [Meninjau kontrol inti](#)
- [Meninjau kontrol standar](#)
- [Meninjau kontrol khusus](#)
- [Membuat kontrol khusus di AWS Audit Manager](#)
 - [Membuat kontrol khusus dari awal di AWS Audit Manager](#)
 - [Membuat salinan kontrol yang dapat diedit di AWS Audit Manager](#)
- [Mengedit kontrol khusus di AWS Audit Manager](#)
- [Mengubah seberapa sering kontrol mengumpulkan bukti](#)
- [Menghapus kontrol khusus di AWS Audit Manager](#)
- [Jenis sumber data yang didukung untuk bukti otomatis](#)
 - [Aturan AWS Config didukung oleh AWS Audit Manager](#)
 - [AWS Security Hub CSPM kontrol didukung oleh AWS Audit Manager](#)
 - [AWS Panggilan API didukung oleh AWS Audit Manager](#)
 - [AWS CloudTrail nama acara didukung oleh AWS Audit Manager](#)

Menemukan kontrol yang tersedia di AWS Audit Manager

Anda dapat menemukan semua kontrol yang tersedia di halaman Control library di konsol Audit Manager.

Anda juga dapat melihat semua kontrol yang tersedia menggunakan Audit Manager API atau AWS Command Line Interface (AWS CLI).

Prasyarat

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk melihat kontrol. AWS

Audit Manager Dua kebijakan yang disarankan yang memberikan izin ini adalah

[AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Audit Manager console

Untuk melihat kontrol yang tersedia di konsol Audit Manager

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.
2. Di panel navigasi, pilih Control library.
3. Pilih tab untuk menelusuri kontrol yang tersedia.
 - Pilih Umum untuk melihat kontrol umum yang disediakan oleh AWS.
 - Pilih Standar untuk melihat kontrol standar yang disediakan oleh AWS.
 - Pilih Kustom untuk melihat kontrol kustom yang Anda buat.

AWS CLI

Untuk menemukan kontrol umum di (AWS CLI

Jalankan [list-common-controls](#) perintah untuk melihat daftar kontrol umum.

```
aws controlcatalog list-common-controls
```

Anda juga dapat menggunakan `common-control-filter` atribut opsional untuk mengembalikan daftar kontrol umum yang memiliki tujuan tertentu.

Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri.

```
aws controlcatalog list-common-controls --common-control-filter OBJECTIVE-ARN
```

Untuk menemukan jenis kontrol lain di AWS CLI

Jalankan perintah [daftar-kontrol](#) dan tentukan `--control-type` sebagai `Custom`, `Standard`, atau `Core`

Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri.

```
aws auditmanager list-controls --control-type Type
```

Audit Manager API

Untuk menemukan kontrol umum menggunakan API

Gunakan [ListCommonControls](#) operasi untuk melihat daftar kontrol umum yang tersedia. Anda juga dapat menggunakan `commonControlFilter` atribut opsional untuk mengembalikan daftar kontrol yang memiliki tujuan tertentu.

Untuk menemukan jenis kontrol lain menggunakan API

Gunakan [ListControls](#) operasi dan tentukan [ControlType](#) sebagai `Custom`, `Standard`, atau `Core`.

Untuk informasi selengkapnya, pilih salah satu tautan di prosedur sebelumnya untuk membaca selengkapnya di Referensi AWS Audit Manager API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu bahasa khusus AWS SDKs.

Langkah selanjutnya

Saat Anda siap untuk menjelajahi detail kontrol, ikuti langkah-langkahnya [Meninjau kontrol di AWS Audit Manager](#). Halaman ini akan memandu Anda melalui detail kontrol dan menjelaskan informasi yang Anda lihat di sana.

Dari halaman pustaka kontrol, Anda juga dapat [membuat kontrol kustom](#), [mengedit kontrol kustom](#), atau [menghapus kontrol kustom](#).

Sumber daya tambahan

Untuk solusi untuk mengontrol masalah di Audit Manager lihat [Memecahkan masalah kontrol dan pengaturan kontrol](#).

Meninjau kontrol di AWS Audit Manager

Anda dapat meninjau detail kontrol menggunakan konsol Audit Manager, Audit Manager API, atau AWS Command Line Interface (AWS CLI).

Untuk memulai meninjau kontrol di Audit Manager, ikuti prosedur yang diuraikan di sini.

- [Meninjau kontrol umum](#)

- [Meninjau kontrol inti](#)
- [Meninjau kontrol standar](#)
- [Meninjau kontrol khusus](#)

Meninjau kontrol umum

Saat Anda perlu meninjau detail kontrol, Anda akan menemukan informasi yang disusun menjadi beberapa bagian di halaman detail kontrol. Bagian ini membantu Anda dengan mudah mengakses dan memahami informasi yang relevan untuk kontrol itu.

Prasyarat

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk melihat kontrol umum di Audit Manager. Lebih khusus lagi, Anda memerlukan izin berikut untuk melihat kontrol umum, tujuan kontrol, dan domain kontrol yang disediakan oleh Katalog AWS Kontrol:

- `controlcatalog:ListCommonControls`
- `controlcatalog:ListDomains`
- `controlcatalog:ListObjectives`

Kebijakan yang disarankan yang memberikan izin ini adalah. [AWSAuditManagerAdministratorAccess](#)

Prosedur

Anda dapat meninjau kontrol umum menggunakan konsol Audit Manager, AWS Control Catalog API, atau AWS Command Line Interface (AWS CLI).

Audit Manager console

Untuk melihat detail kontrol umum di konsol Audit Manager

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.
2. Di panel navigasi, pilih Control library.
3. Pilih Umum untuk melihat kontrol umum yang disediakan oleh AWS.
4. Pilih nama kontrol umum untuk melihat detail untuk kontrol itu.

5. Tinjau detail kontrol umum menggunakan informasi berikut sebagai referensi.

Bagian ikhtisar

Bagian ini menjelaskan kontrol umum.

Tab sumber bukti

Tab ini mencakup informasi berikut:

Nama	Deskripsi
Kontrol inti	Ini adalah kontrol inti yang mengumpulkan bukti untuk mendukung kontrol bersama. • Ketika Anda mengumpulkan bukti untuk kontrol umum ini, Anda secara otomatis mengumpulkan bukti untuk semua kontrol inti yang tercantum di sini. Ketika masing-masing kontrol inti ini diimplementasikan dengan sukses, ini membantu menunjukkan bahwa Anda memenuhi persyaratan kontrol umum. • Setiap kontrol inti menggunakan pengelompokan sumber data yang telah ditentukan sebelumnya untuk mengumpulkan bukti tentang suatu. Layanan AWS AWS mengelola sumber data ini untuk Anda. Ini berarti bahwa mereka diperbarui secara otomatis setiap kali peraturan dan standar berubah dan sumber data baru diidentifikasi. Pilih kontrol inti apa pun untuk melihat sumber data yang mendasarinya.

Tab persyaratan terkait

Saat Anda mengumpulkan bukti untuk kontrol umum ini, bukti yang sama dapat membantu Anda menunjukkan kepatuhan terhadap persyaratan kontrol standar terkait yang tercantum di tab ini. Pilih kontrol standar apa pun untuk melihat detail lebih lanjut.

Note

- Kontrol umum mungkin menghasilkan bukti yang menunjukkan hanya kepatuhan sebagian dengan kontrol standar. Ada kemungkinan bahwa Anda mungkin

memerlukan bukti tambahan untuk menunjukkan kepatuhan penuh terhadap kontrol standar.

- Pada saat ini, tab Persyaratan terkait hanya menampilkan kontrol standar terkait. Meskipun kontrol umum dapat dikaitkan dengan satu atau beberapa kontrol kustom, hubungan tersebut tidak ditampilkan di tab ini.

AWS CLI

Untuk melihat detail kontrol umum di AWS CLI

1. Jalankan [list-common-controls](#) perintah untuk melihat daftar kontrol umum yang tersedia. Saat Anda menggunakan operasi ini, Anda dapat menerapkan opsional `common-control-filter` untuk melihat kontrol umum yang memiliki tujuan tertentu.

```
aws controlcatalog list-common-controls
```

2. Dalam tanggapannya, identifikasi kontrol umum yang ingin Anda tinjau dan catat detailnya.

AWS Control Catalog API

Untuk melihat detail kontrol umum menggunakan API

1. Gunakan [ListCommonControls](#) operasi untuk melihat daftar kontrol umum yang tersedia. Bila Anda menggunakan operasi ini, Anda dapat menerapkan opsional `commonControlFilter` untuk melihat daftar kontrol yang memiliki tujuan tertentu.
2. Dalam tanggapannya, identifikasi kontrol yang ingin Anda tinjau dan catat detailnya.

Untuk informasi selengkapnya tentang operasi API ini, pilih tautan dalam prosedur ini untuk membaca selengkapnya di Referensi API Katalog AWS Kontrol. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu bahasa khusus AWS SDKs.

Langkah selanjutnya

Anda dapat memilih kontrol umum yang mewakili tujuan Anda dan menggunakannya sebagai blok bangunan untuk membuat kontrol khusus. Setiap peta kontrol umum otomatis ke pengelompokan sumber AWS data yang telah ditentukan sebelumnya yang ditangani Audit Manager untuk

Anda. Ini berarti Anda tidak harus menjadi AWS ahli untuk mengetahui sumber data mana yang mengumpulkan bukti yang relevan untuk tujuan Anda. Selain itu, Anda tidak perlu memelihara pemetaan sumber data ini sendiri.

Untuk petunjuk tentang cara membuat kontrol kustom yang menggunakan kontrol umum sebagai sumber bukti, lihat [Membuat kontrol khusus di AWS Audit Manager](#).

Sumber daya tambahan

- [Meninjau kontrol inti](#)
- [Meninjau kontrol standar](#)
- [Meninjau kontrol khusus](#)

Meninjau kontrol inti

Anda dapat meninjau detail kontrol inti menggunakan konsol Audit Manager, Audit Manager API, atau AWS Command Line Interface (AWS CLI).

Prasyarat

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk melihat kontrol. AWS Audit Manager Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Audit Manager console

Untuk melihat detail kontrol inti di konsol Audit Manager

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.
2. Di panel navigasi, pilih Control library.
3. Pilih Umum untuk melihat kontrol umum yang disediakan oleh AWS.
4. Cari kontrol umum yang memenuhi kasus penggunaan Anda.
5. Pilih ikon tampilan pohon di sebelah nama kontrol umum. Ini menampilkan kontrol inti yang mendukung kontrol umum.

6. Pilih nama kontrol inti yang ingin Anda tinjau.
7. Tinjau detail kontrol inti menggunakan informasi berikut sebagai referensi.

Bagian ikhtisar

Bagian ini menjelaskan kontrol inti dan mencantumkan [tipe sumber data](#) tempat ia mengumpulkan bukti.

Tab sumber bukti

Tab ini mencakup informasi berikut:

Nama	Deskripsi
Sumber data	Ini adalah sumber data AWS terkelola tempat kontrol inti mengumpulkan bukti. Sumber data ini diperbarui secara otomatis setiap kali peraturan dan standar berubah dan sumber data baru diidentifikasi. • Pemetaan — Kata kunci spesifik yang digunakan untuk mengumpulkan bukti. • Jika jenisnya AWS Config, pemetaan adalah AWS Config aturan (seperti <code>SNS_ENCRYPTED_KMS</code>). • Jika jenisnya AWS Security Hub CSPM, pemetaan adalah kontrol CSPM Security Hub (seperti). <code>EC2.1</code> • Jika jenisnya adalah panggilan AWS API, pemetaan adalah panggilan API (seperti <code>kms_ListKeys</code>). • Jika jenisnya AWS CloudTrail, pemetaan adalah CloudTrail peristiwa (seperti <code>CreateAccessKey</code>). • Jenis — Jenis sumber data tempat bukti berasal. • Jika Audit Manager mengumpulkan bukti, jenisnya bisa berupa AWS Security Hub CSPM, AWS ConfigAWS CloudTrail, atau panggilan AWS API. • Jika Anda mengunggah bukti Anda sendiri, jenisnya adalah Manual. Deskripsi menunjukkan apakah bukti manual yang diperlukan adalah unggahan File atau respons Teks.

Nama	Deskripsi
	Frekuensi — Seberapa sering Audit Manager mengumpulkan bukti untuk sumber data panggilan AWS API.

Tab Detail

Tab ini mencakup informasi berikut:

Nama	Deskripsi
Instruksi	Petunjuk yang menjelaskan cara menguji dan memulihkan kontrol.
Menguji informasi	Prosedur pengujian yang direkomendasikan.
Rencana aksi	Tindakan yang disarankan untuk diambil jika Anda perlu memulihkan kontrol.

AWS CLI

Untuk melihat detail kontrol inti di AWS CLI

- Ikuti langkah-langkah untuk [menemukan kontrol](#). Pastikan untuk mengatur `--control-type asCore`, dan menerapkan filter opsional sesuai kebutuhan.

```
aws auditmanager list-controls --control-type Core
```

- Sebagai tanggapan, identifikasi kontrol yang ingin Anda tinjau dan catat ID kontrol dan Nama Sumber Daya Amazon (ARN).
- Jalankan perintah [get-control](#) dan tentukan. `--control-id` Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

 Tip

Rincian kontrol dikembalikan dalam format JSON. Untuk membantu Anda memahami data ini, lihat [Get-control Output](#) di AWS CLI Command Reference.

4. Untuk melihat detail tag, jalankan [list-tags-for-resource](#) perintah dan tentukan `--resource-arn`. Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri.

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

Untuk melihat detail kontrol inti menggunakan API

1. Ikuti langkah-langkah untuk [menemukan kontrol](#). Pastikan untuk mengatur [ControlType](#) sebagai `Core`, dan menerapkan filter opsional sesuai kebutuhan.
2. Sebagai tanggapan, identifikasi kontrol yang ingin Anda tinjau dan catat ID kontrol dan Nama Sumber Daya Amazon (ARN).
3. Gunakan [GetControl](#) operasi dan tentukan [ControlId](#) yang Anda catat di langkah 2.

 Tip

Rincian kontrol dikembalikan dalam format JSON. Untuk membantu Anda memahami data ini, lihat [Elemen GetControl Respons](#) di Referensi AWS Audit Manager API.

4. Untuk melihat detail tag, gunakan [ListTagsForResource](#) operasi dan tentukan [ResourceArn](#) yang Anda catat di langkah 2.

Untuk informasi selengkapnya tentang operasi API ini, pilih salah satu tautan dalam prosedur ini untuk membaca selengkapnya di Referensi AWS Audit Manager API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu bahasa khusus AWS SDKs.

Langkah selanjutnya

Anda dapat memilih kontrol inti yang mewakili tujuan Anda dan menggunakannya sebagai blok bangunan untuk membuat kontrol khusus. Setiap kontrol inti otomatis memetakan ke pengelompokan sumber AWS data yang telah ditentukan sebelumnya yang ditangani Audit Manager untuk Anda. Ini berarti Anda tidak harus menjadi AWS ahli untuk mengetahui sumber data mana yang mengumpulkan bukti yang relevan untuk tujuan Anda. Selain itu, Anda tidak perlu memelihara pemetaan sumber data ini sendiri.

Untuk petunjuk tentang cara membuat kontrol kustom yang menggunakan kontrol inti sebagai sumber bukti, lihat [Membuat kontrol khusus di AWS Audit Manager](#).

Sumber daya tambahan

- [Meninjau kontrol umum](#)
- [Meninjau kontrol standar](#)
- [Meninjau kontrol khusus](#)

Meninjau kontrol standar

Anda dapat meninjau detail kontrol standar menggunakan konsol Audit Manager, Audit Manager API, atau AWS Command Line Interface (AWS CLI).

Prasyarat

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk melihat kontrol. AWS Audit Manager Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Anda dapat meninjau detail kontrol standar menggunakan konsol Audit Manager, Audit Manager API, atau AWS Command Line Interface (AWS CLI).

Audit Manager console

Untuk melihat detail kontrol standar di konsol Audit Manager

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.
2. Di panel navigasi, pilih Control library.
3. Pilih Standar untuk melihat kontrol standar yang disediakan oleh AWS.
4. Pilih nama kontrol standar apa pun untuk melihat detail untuk kontrol itu.
5. Tinjau detail kontrol standar menggunakan informasi berikut sebagai referensi.

Bagian ikhtisar

Bagian ini menjelaskan kontrol standar dan mencantumkan [tipe sumber data](#) yang digunakannya untuk mengumpulkan bukti.

Tab sumber bukti

Tab ini mencakup informasi berikut:

Nama	Deskripsi
Kontrol inti	Ini adalah kontrol inti yang mengumpulkan bukti untuk mendukung kontrol standar. Setiap kontrol inti menggunakan pengelompokan sumber data yang telah ditentukan sebelumnya untuk mengumpulkan bukti tentang suatu. Layanan AWS Sumber data ini dikelola untuk Anda oleh AWS, dan diperbarui secara otomatis setiap kali peraturan dan standar berubah dan sumber data baru diidentifikasi. Pilih kontrol inti apa pun untuk melihat sumber data yang mendasarinya.
Sumber data	Ini adalah sumber data AWS terkelola lainnya yang mengumpulkan bukti untuk mendukung kontrol standar. • Pemetaan — Kata kunci spesifik yang digunakan untuk mengumpulkan bukti. • Jika jenisnya AWS Config, pemetaan adalah AWS Config aturan (seperti <code>SNS_ENCRYPTED_KMS</code>).

Nama	Deskripsi
	• Jika jenisnya AWS Security Hub CSPM, pemetaan adalah kontrol CSPM Security Hub (seperti). EC2 . 1 • Jika jenisnya adalah panggilan AWS API, pemetaan adalah panggilan API (seperti <code>kms_ListKeys</code>). • Jika jenisnya AWS CloudTrail, pemetaan adalah CloudTrail peristiwa (seperti <code>CreateAccessKey</code>). • Jenis — Jenis sumber data tempat bukti berasal. • Jika Audit Manager mengumpulkan bukti, jenisnya bisa berupa AWS Security Hub CSPM, AWS Config AWS CloudTrail, atau panggilan AWS API. • Jika Anda mengunggah bukti Anda sendiri, jenisnya adalah Manual. Deskripsi menunjukkan apakah bukti manual yang diperlukan adalah unggahan File atau respons Teks. • Frekuensi — Seberapa sering Audit Manager mengumpulkan bukti untuk sumber data panggilan AWS API.

Tab Detail

Tab ini mencakup informasi berikut:

Nama	Deskripsi
Instruksi	Petunjuk yang menjelaskan cara menguji dan memulihkan kontrol.
Menguji informasi	Prosedur pengujian yang direkomendasikan.
Rencana aksi	Tindakan yang disarankan untuk diambil jika Anda perlu memulihkan kontrol.
Tanda	Tag yang terkait dengan kontrol.

Nama	Deskripsi
Kunci	Kunci tag (misalnya, standar kepatuhan, peraturan, atau kategori).
Nilai	Nilai tanda.

AWS CLI

Untuk melihat detail kontrol standar di AWS CLI

1. Ikuti langkah-langkah untuk [menemukan kontrol](#). Pastikan untuk mengatur `--control-type asStandard`, dan menerapkan filter opsional sesuai kebutuhan.

```
aws auditmanager list-controls --control-type Standard
```

2. Sebagai tanggapan, identifikasi kontrol yang ingin Anda tinjau dan catat ID kontrol dan Nama Sumber Daya Amazon (ARN).
3. Jalankan perintah [get-control](#) dan tentukan. `--control-id` Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Tip

Rincian kontrol dikembalikan dalam format JSON. Untuk membantu Anda memahami data ini, lihat [Get-control Output](#) di Command Reference AWS CLI

4. Untuk melihat detail tag, jalankan [list-tags-for-resource](#) perintah dan tentukan `--resource-arn`. Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri.

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

Untuk melihat detail kontrol standar menggunakan API

1. Ikuti langkah-langkah untuk [menemukan kontrol](#). Pastikan untuk mengatur [ControlType](#) sebagai `Standard`, dan menerapkan filter opsional sesuai kebutuhan.
2. Sebagai tanggapan, identifikasi kontrol yang ingin Anda tinjau dan catat ID kontrol dan Nama Sumber Daya Amazon (ARN).
3. Gunakan [GetControl](#) operasi dan tentukan [ControlId](#) yang Anda catat di langkah 2.

Tip

Rincian kontrol dikembalikan dalam format JSON. Untuk membantu Anda memahami data ini, lihat [Elemen GetControl Respons](#) di Referensi AWS Audit Manager API.

4. Untuk melihat detail tag, gunakan [ListTagsForResource](#) operasi dan tentukan [ResourceArn](#) yang Anda catat di langkah 2.

Untuk informasi selengkapnya tentang operasi API ini, pilih salah satu tautan dalam prosedur ini untuk membaca selengkapnya di Referensi AWS Audit Manager API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu bahasa khusus AWS SDKs.

Langkah selanjutnya

Anda dapat menambahkan kontrol standar ke salah satu kerangka kerja kustom Anda. Untuk petunjuk, lihat [Membuat kerangka kerja khusus di AWS Audit Manager](#).

Anda juga dapat menyesuaikan kontrol standar apa pun sehingga memenuhi kebutuhan Anda. Untuk petunjuk, lihat [Membuat salinan kontrol yang dapat diedit di AWS Audit Manager](#).

Sumber daya tambahan

- [Meninjau kontrol umum](#)
- [Meninjau kontrol inti](#)
- [Meninjau kontrol khusus](#)

Meninjau kontrol khusus

Anda dapat meninjau detail kontrol kustom menggunakan konsol Audit Manager, Audit Manager API, atau AWS Command Line Interface (AWS CLI).

Prasyarat

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk melihat kontrol. AWS Audit Manager Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Anda dapat meninjau detail kontrol kustom menggunakan konsol Audit Manager, Audit Manager API, atau AWS Command Line Interface (AWS CLI).

Audit Manager console

Untuk melihat detail kontrol kustom di konsol Audit Manager

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.
2. Di panel navigasi, pilih Control library.
3. Pilih Kustom untuk melihat kontrol kustom yang Anda buat.
4. Pilih nama kontrol khusus apa pun untuk melihat detail untuk kontrol itu.
5. Tinjau detail kontrol kustom menggunakan informasi berikut sebagai referensi.

Bagian ikhtisar

Bagian ini menjelaskan kontrol khusus dan mencantumkan [tipe sumber data](#) yang digunakannya untuk mengumpulkan bukti. Ini juga memberikan informasi tentang kapan kontrol dibuat dan terakhir diperbarui.

Tab sumber bukti

Tab ini menunjukkan dari mana kontrol kustom mengumpulkan bukti. Ini termasuk informasi berikut:

Nama	Deskripsi
Kontrol umum	Ini adalah kontrol umum yang mengumpulkan bukti untuk mendukung kontrol kustom. Kontrol umum mengumpulkan bukti menggunakan sumber data dasar yang AWS mengelola untuk Anda. Untuk setiap kontrol umum yang terdaftar, Audit Manager mengumpulkan bukti yang relevan untuk semua kontrol inti pendukung. Pilih kontrol umum untuk melihat kontrol inti terkait.
Kontrol inti	Ini adalah kontrol inti yang mengumpulkan bukti untuk mendukung kontrol kustom. Kontrol inti mengumpulkan bukti dengan menggunakan kelompok sumber data yang telah ditentukan sebelumnya yang AWS mengelola untuk Anda. Pilih kontrol inti untuk melihat sumber data yang mendasarinya.
Sumber data	Ini adalah sumber data yang mengumpulkan bukti untuk mendukung kontrol kustom.  Note Sumber data ini tidak dikelola untuk Anda oleh AWS. Anda bertanggung jawab untuk mempertahankannya. • Nama — Nama sumber data. • Jenis — Jenis sumber data tempat bukti berasal. • Jika Audit Manager mengumpulkan bukti, jenisnya bisa berupa AWS Security Hub CSPM, AWS Config, AWS CloudTrail, atau panggilan AWS API. • Jika Anda mengunggah bukti Anda sendiri, jenisnya adalah Manual. Deskripsi menunjukkan apakah bukti manual yang diperlukan adalah unggahan File atau respons Teks.

Nama	Deskripsi
	• Pemetaan — Kata kunci spesifik yang digunakan untuk mengumpulkan bukti. • Jika jenisnya AWS Config, pemetaan adalah AWS Config aturan (seperti <code>SNS_ENCRYPTED_KMS</code>). • Jika jenisnya AWS Security Hub CSPM, pemetaan adalah kontrol CSPM Security Hub (seperti). <code>EC2.1</code> • Jika jenisnya adalah panggilan AWS API, pemetaan adalah panggilan API (seperti <code>kms_ListKeys</code>). • Jika jenisnya AWS CloudTrail, pemetaan adalah CloudTrail peristiwa (seperti <code>CreateAccessKey</code>). • Frekuensi — Seberapa sering Audit Manager mengumpulkan bukti untuk sumber data panggilan AWS API.

Tab Detail

Tab ini mencakup informasi berikut:

Nama	Deskripsi
Instruksi	Petunjuk yang menjelaskan cara menguji dan memulihkan kontrol.
Menguji informasi	Prosedur pengujian yang direkomendasikan.
Rencana aksi	Tindakan yang disarankan untuk diambil jika Anda perlu memulihkan kontrol.
Tanda	Tag yang terkait dengan kontrol.
Kunci	Kunci tag (misalnya, standar kepatuhan, peraturan, atau kategori).
Nilai	Nilai tanda.

AWS CLI

Untuk melihat detail kontrol kustom di AWS CLI

1. Ikuti langkah-langkah untuk [menemukan kontrol](#). Pastikan untuk mengatur `--control-type` asCustom, dan menerapkan filter opsional sesuai kebutuhan.

```
aws auditmanager list-controls --control-type Custom
```

2. Sebagai tanggapan, identifikasi kontrol yang ingin Anda tinjau dan catat ID kontrol dan Nama Sumber Daya Amazon (ARN).
3. Jalankan perintah [get-control](#) dan tentukan. `--control-id` Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Tip

Rincian kontrol dikembalikan dalam format JSON. Untuk membantu Anda memahami data ini, lihat [Get-control Output](#) di AWS CLI Command Reference.

4. Untuk melihat tag untuk kontrol, gunakan [list-tags-for-resource](#) perintah dan tentukan `--resource-arn`. Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri:

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

Untuk melihat detail kontrol kustom menggunakan API

1. Ikuti langkah-langkah untuk [menemukan kontrol](#). Pastikan untuk mengatur [ControlType](#) sebagaiCustom, dan menerapkan filter opsional sesuai kebutuhan.
2. Sebagai tanggapan, identifikasi kontrol yang ingin Anda tinjau dan catat ID kontrol dan Nama Sumber Daya Amazon (ARN).
3. Gunakan [GetControl](#) operasi dan tentukan [ControlId](#) yang Anda catat di langkah 2.

 Tip

Rincian kontrol dikembalikan dalam format JSON. Untuk membantu Anda memahami data ini, lihat [Elemen GetControl Respons](#) di Referensi AWS Audit Manager API.

4. Untuk melihat tag untuk kontrol, gunakan [ListTagsForResource](#) operasi dan tentukan kontrol [ResourceArn](#) yang Anda catat di langkah 2.

Untuk informasi selengkapnya tentang operasi API ini, pilih salah satu tautan dalam prosedur ini untuk membaca selengkapnya di Referensi AWS Audit Manager API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu bahasa khusus AWS SDKs.

Langkah selanjutnya

Anda dapat menambahkan kontrol khusus ke salah satu kerangka kerja kustom Anda. Untuk petunjuk, lihat [Membuat kerangka kerja khusus di AWS Audit Manager](#).

Anda juga dapat [mengedit kontrol kustom](#), [membuat salinan kontrol kustom yang dapat diedit](#), atau [menghapus kontrol khusus yang](#) tidak lagi Anda perlukan.

Sumber daya tambahan

- [Meninjau kontrol umum](#)
- [Meninjau kontrol inti](#)
- [Meninjau kontrol standar](#)

Membuat kontrol khusus di AWS Audit Manager

Anda dapat menggunakan kontrol khusus untuk mengumpulkan bukti untuk kebutuhan kepatuhan spesifik Anda.

Sama seperti kontrol standar, kontrol kustom mengumpulkan bukti terus-menerus ketika mereka aktif dalam penilaian Anda. Anda juga dapat menambahkan bukti manual ke kontrol kustom apa pun yang Anda buat. Setiap bukti menjadi catatan yang membantu Anda menunjukkan kepatuhan terhadap persyaratan kontrol kustom Anda.

Untuk memulai, berikut adalah beberapa contoh bagaimana Anda dapat menggunakan kontrol khusus:

Memetakan kontrol perusahaan Anda ke pengelompokan sumber data yang telah ditentukan AWS

Anda dapat melakukan onboard kontrol perusahaan ke Audit Manager dengan menggunakan kontrol umum sebagai sumber bukti. Pilih kontrol umum yang mewakili tujuan Anda, dan gunakan sebagai blok bangunan untuk membuat kontrol yang mengumpulkan bukti di seluruh portofolio kebutuhan kepatuhan Anda. Setiap peta kontrol umum otomatis ke pengelompokan sumber data yang telah ditentukan sebelumnya. Ini berarti Anda tidak harus menjadi AWS ahli untuk mengetahui sumber data mana yang mengumpulkan bukti yang relevan untuk tujuan Anda. Dan ketika Anda menggunakan kontrol umum sebagai sumber bukti, Anda tidak perlu lagi memelihara pemetaan sumber data, karena Audit Manager menangani ini untuk Anda.

Buat pertanyaan penilaian risiko vendor

Anda dapat menggunakan kontrol khusus untuk mendukung cara Anda mengelola penilaian risiko vendor. Setiap kontrol yang Anda buat dapat mewakili pertanyaan penilaian risiko individu. Misalnya, nama kontrol dapat berupa pertanyaan, dan Anda dapat memberikan jawaban dengan mengunggah file atau memasukkan respons teks sebagai bukti manual.

Poin kunci

Ketika datang untuk membuat kontrol kustom di Audit Manager, Anda memiliki dua metode untuk dipilih:

1. Membuat kontrol dari awal - Metode ini memberikan fleksibilitas maksimum dan memungkinkan Anda untuk menyesuaikan kontrol dengan kebutuhan Anda yang tepat. Ini adalah pilihan yang baik ketika Anda memiliki persyaratan kepatuhan khusus yang tidak tercakup secara memadai oleh kontrol yang ada. Metode ini sangat berguna ketika Anda perlu memetakan kontrol perusahaan organisasi Anda ke pengelompokan sumber AWS data yang telah ditentukan sebelumnya atau ketika Anda ingin membuat pertanyaan penilaian risiko vendor sebagai kontrol individu.
2. Membuat salinan kontrol yang ada yang dapat diedit - Jika kontrol standar atau kontrol khusus yang ada sebagian memenuhi kebutuhan Anda, Anda dapat membuat salinan kontrol yang dapat diedit. Pendekatan ini lebih efisien jika Anda hanya perlu membuat perubahan kecil pada kontrol yang ada. Ini adalah opsi yang baik jika Anda ingin menyesuaikan beberapa atribut untuk menyelaraskan kontrol dengan persyaratan spesifik Anda dengan lebih baik. Misalnya, Anda dapat

mengubah seberapa sering kontrol menggunakan panggilan API untuk mengumpulkan bukti, lalu mengubah nama kontrol untuk mencerminkan hal ini.

Sumber daya tambahan

Untuk petunjuk tentang cara membuat kontrol kustom, lihat sumber daya berikut.

- [Membuat kontrol khusus dari awal di AWS Audit Manager](#)
- [Membuat salinan kontrol yang dapat diedit di AWS Audit Manager](#)

Membuat kontrol khusus dari awal di AWS Audit Manager

Jika persyaratan kepatuhan organisasi Anda tidak selaras dengan kontrol standar bawaan yang tersedia AWS Audit Manager, Anda dapat membuat kontrol kustom sendiri dari awal.

Halaman ini menguraikan langkah-langkah untuk membuat kontrol khusus yang disesuaikan dengan kebutuhan spesifik Anda.

Prasyarat

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk membuat kontrol khusus. AWS Audit Manager Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Agar berhasil mengumpulkan bukti dari AWS Config dan Security Hub CSPM, pastikan Anda melakukan hal berikut:

- [Aktifkan AWS Config](#), lalu terapkan [pengaturan yang diperlukan untuk digunakan AWS Config dengan Audit Manager](#)
- [Aktifkan Security Hub CSPM](#), lalu terapkan [pengaturan yang diperlukan untuk menggunakan Security Hub CSPM](#) dengan Audit Manager

Audit Manager kemudian dapat mengumpulkan bukti setiap kali evaluasi terjadi untuk AWS Config aturan tertentu atau kontrol CSPM Security Hub.

Prosedur

Tugas

- [Langkah 1: Tentukan detail kontrol](#)
- [Langkah 2: Tentukan sumber bukti](#)
- [Langkah 3 \(Opsional\): Tentukan rencana tindakan](#)
- [Langkah 4: Tinjau dan buat kontrol](#)

Langkah 1: Tentukan detail kontrol

Mulailah dengan menentukan detail kontrol kustom Anda.

Important

Kami sangat menyarankan agar Anda tidak pernah memasukkan informasi identifikasi sensitif ke dalam bidang bentuk bebas seperti detail Kontrol atau informasi Pengujian. Jika Anda membuat kontrol khusus yang berisi informasi sensitif, Anda tidak dapat membagikan kerangka kerja kustom apa pun yang berisi kontrol ini.

Untuk menentukan detail kontrol

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.
2. Di panel navigasi, pilih Control library, lalu pilih Create custom control.
3. Di bawah Detail kontrol, masukkan informasi berikut tentang kontrol.
 - Kontrol — Masukkan nama ramah, judul, atau pertanyaan penilaian risiko. Nilai ini membantu Anda mengidentifikasi kontrol Anda di pustaka kontrol.
 - Deskripsi (opsional) — Masukkan detail untuk membantu orang lain memahami tujuan kontrol. Deskripsi ini muncul di halaman detail kontrol.
4. Di bawah Informasi pengujian, masukkan langkah-langkah yang disarankan untuk menguji kontrol.
5. Di bawah Tag, pilih Tambahkan tag baru untuk mengaitkan tag dengan kontrol. Anda dapat menentukan kunci untuk setiap tag yang paling menggambarkan kerangka kepatuhan yang didukung kontrol ini. Kunci tag adalah wajib dan dapat digunakan sebagai kriteria pencarian saat Anda mencari kontrol ini di pustaka kontrol.

6. Pilih Berikutnya.

Langkah 2: Tentukan sumber bukti

Selanjutnya, tentukan beberapa sumber bukti. Sumber bukti menentukan dari mana kontrol kustom Anda mengumpulkan bukti. Anda dapat menggunakan sumber AWS terkelola, sumber yang dikelola pelanggan, atau keduanya.

Tip

Kami menyarankan Anda menggunakan sumber AWS terkelola. Setiap kali sumber AWS terkelola diperbarui, pembaruan yang sama secara otomatis diterapkan ke semua kontrol khusus yang menggunakan sumber ini. Ini berarti bahwa kontrol kustom Anda mengumpulkan bukti terhadap definisi terbaru dari sumber bukti tersebut.

Jika Anda tidak yakin opsi mana yang harus dipilih, lihat contoh berikut dan rekomendasi kami.

Peran Anda	Tujuan Anda	Sumber bukti yang direkomendasikan
GRC profesional	Saya ingin mengumpulkan bukti untuk domain atau tujuan tertentu	AWS dikelola (common control) Gunakan pengelompokan sumber data yang telah ditentukan sebelumnya yang memetakan ke kontrol umum tertentu.
Pakar teknis	Saya ingin mengumpulkan bukti tentang AWS sumber daya yang menjadi tanggung jawab saya	AWS dikelola (core control) Gunakan pengelompokan sumber data yang telah ditentukan sebelumnya yang memetakan ke suatu AWS persyaratan.

Peran Anda	Tujuan Anda	Sumber bukti yang direkomen dasikan
Pakar teknis	Saya ingin menggunakan AWS Config aturan khusus untuk mengumpulkan bukti	Dikelola pelanggan (Otomatis data source) Gunakan sumber data khusus untuk mengumpulkan bukti otomatis tertentu.
GRC profesional	Saya ingin mengumpulkan bukti, seperti dokumen dan tanggapan teks	Pelanggan dikelola (Manual data source) Gunakan sumber data khusus untuk mengunggah bukti manual Anda sendiri.

Untuk menentukan sumber AWS terkelola (disarankan)

Kami menyarankan Anda memulai dengan memilih satu atau lebih kontrol umum. Ketika Anda memilih kontrol umum yang mewakili tujuan Anda, Audit Manager mengumpulkan bukti yang relevan untuk semua kontrol inti pendukung. Anda juga dapat memilih kontrol inti individu jika Anda ingin mengumpulkan bukti yang ditargetkan tentang AWS lingkungan Anda.

Untuk menentukan sumber AWS terkelola

1. Buka bagian sumber AWS terkelola halaman.
2. Untuk menambahkan kontrol umum, ikuti langkah-langkah ini:
 - a. Pilih Gunakan kontrol umum yang sesuai dengan sasaran kepatuhan Anda.
 - b. Pilih kontrol umum dari daftar dropdown.
 - c. (Opsional) Ulangi langkah 2 sesuai kebutuhan. Anda dapat menambahkan hingga lima kontrol umum.
3. Untuk menghapus kontrol umum, pilih X di sebelah nama kontrol.
4. Untuk menambahkan kontrol inti, ikuti langkah-langkah ini:
 - a. Pilih Gunakan kontrol inti yang cocok dengan pedoman preskriptif AWS .

- b. Pilih kontrol umum dari daftar dropdown.
 - c. (Opsional) Ulangi langkah 4 sesuai kebutuhan. Anda dapat menambahkan hingga 50 kontrol inti.
5. Untuk menghapus kontrol inti, pilih X di sebelah nama kontrol.
6. Untuk menambahkan sumber data yang dikelola pelanggan, gunakan prosedur berikut. Jika tidak, pilih Selanjutnya.

Untuk menentukan sumber terkelola pelanggan

Untuk mengumpulkan bukti otomatis dari sumber data, Anda harus memilih tipe sumber data dan pemetaan sumber data. Detail ini dipetakan ke AWS penggunaan Anda, dan beri tahu Audit Manager tempat mengumpulkan bukti. Jika Anda ingin memberikan bukti Anda sendiri, Anda akan memilih sumber data manual sebagai gantinya.

Note

Anda bertanggung jawab untuk menjaga pemetaan sumber data yang Anda buat di langkah ini.

Untuk menentukan sumber terkelola pelanggan

1. Buka bagian Sumber terkelola pelanggan di halaman.
2. Pilih Gunakan sumber data untuk mengumpulkan bukti manual atau otomatis.
3. Pilih Tambahkan.
4. Pilih salah satu opsi berikut:
 - Pilih panggilan AWS API, lalu pilih panggilan API dan frekuensi pengumpulan bukti.
 - Pilih AWS CloudTrail acara, lalu pilih nama acara.
 - Pilih aturan AWS Config terkelola, lalu pilih pengidentifikasi aturan.
 - Pilih aturan AWS Config khusus, lalu pilih pengenalan aturan.
 - Pilih AWS Security Hub CSPM kontrol, lalu pilih kontrol CSPM Security Hub.
 - Pilih Sumber data manual, lalu pilih opsi:
 - Unggah file — Gunakan opsi ini jika kontrol memerlukan dokumentasi sebagai bukti.

- Respons teks — Gunakan opsi ini jika kontrol memerlukan jawaban atas pertanyaan penilaian risiko.

 Tip

Untuk informasi tentang jenis sumber data otomatis dan tips pemecahan masalah, lihat. [Jenis sumber data yang didukung untuk bukti otomatis](#)
Jika Anda perlu memvalidasi penyiapan sumber data Anda dengan pakar, pilih Sumber data manual untuk saat ini. Dengan begitu, Anda dapat membuat kontrol dan menambahkannya ke kerangka kerja sekarang, dan kemudian [mengedit kontrol](#) sesuai kebutuhan nanti.

5. Di bawah Nama sumber data, berikan nama deskriptif.
6. (Opsional) Di bawah Detail tambahan, masukkan deskripsi sumber data dan deskripsi pemecahan masalah.
7. Pilih Tambahkan sumber data.
8. (Opsional) Untuk menambahkan sumber data lain, pilih Tambah dan ulangi langkah 1-7. Anda dapat menambahkan hingga 100 sumber data.
9. Untuk menghapus sumber data, pilih sumber data dari tabel, lalu pilih Hapus.
10. Setelah selesai, pilih Berikutnya.

Langkah 3 (Opsional): Tentukan rencana tindakan

Selanjutnya, tentukan tindakan yang harus diambil jika kontrol ini perlu diperbaiki.

 Important

Kami sangat menyarankan agar Anda tidak pernah memasukkan informasi identifikasi sensitif ke dalam bidang bentuk bebas seperti Rencana tindakan. Jika Anda membuat kontrol khusus yang berisi informasi sensitif, Anda tidak dapat membagikan kerangka kerja kustom apa pun yang berisi kontrol ini.

Untuk menentukan rencana aksi

1. Di bawah Judul, masukkan judul deskriptif untuk rencana tindakan.

2. Di bawah Instruksi, masukkan instruksi terperinci untuk rencana tindakan.
3. Pilih Berikutnya.

Langkah 4: Tinjau dan buat kontrol

Tinjau informasi untuk kontrol. Untuk mengubah informasi untuk satu langkah, pilih Edit.

Setelah selesai, pilih Buat kontrol khusus.

Langkah selanjutnya

Setelah Anda membuat kontrol kustom baru, Anda dapat menambahkannya ke kerangka kustom. Untuk mempelajari lebih lanjut, lihat [Membuat kerangka kerja khusus di AWS Audit Manager](#) atau [Mengedit kerangka kerja khusus di AWS Audit Manager](#).

Setelah Anda menambahkan kontrol kustom ke kerangka kustom, Anda dapat membuat penilaian dan mulai mengumpulkan bukti. Untuk mempelajari selengkapnya, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk meninjau kembali kontrol kustom Anda di kemudian hari, lihat [Menemukan kontrol yang tersedia di AWS Audit Manager](#). Anda dapat mengikuti langkah-langkah ini untuk menemukan kontrol kustom Anda sehingga Anda dapat melihat, mengedit, atau menghapusnya.

Sumber daya tambahan

Untuk solusi untuk mengontrol masalah di Audit Manager, lihat [Memecahkan masalah kontrol dan pengaturan kontrol](#).

Membuat salinan kontrol yang dapat diedit di AWS Audit Manager

Alih-alih membuat kontrol khusus dari awal, Anda dapat menggunakan kontrol standar atau kontrol khusus yang ada sebagai titik awal dan membuat salinan yang dapat diedit yang memenuhi kebutuhan Anda. Saat Anda melakukan ini, kontrol standar yang ada tetap ada di pustaka kontrol, dan kontrol baru dibuat dengan pengaturan kustom Anda.

Prasyarat

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk membuat kerangka kerja khusus. AWS Audit Manager Dua kebijakan yang disarankan yang memberikan izin ini adalah

[AWS Audit Manager Administrator Access](#) dan [izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Agar berhasil mengumpulkan bukti dari AWS Config dan Security Hub CSPM, pastikan Anda melakukan hal berikut:

- [Aktifkan AWS Config](#), lalu terapkan [pengaturan yang diperlukan untuk digunakan AWS Config dengan Audit Manager](#).
- [Aktifkan Security Hub CSPM](#), lalu terapkan [pengaturan yang diperlukan untuk menggunakan Security Hub CSPM dengan Audit Manager](#).

Audit Manager kemudian dapat mengumpulkan bukti setiap kali evaluasi terjadi untuk AWS Config aturan tertentu atau kontrol CSPM Security Hub.

Prosedur

Tugas

- [Langkah 1: Tentukan detail kontrol](#)
- [Langkah 2: Tentukan sumber bukti](#)
- [Langkah 3: \(Opsional\): Tentukan rencana tindakan](#)
- [Langkah 4: Tinjau dan buat kontrol](#)

Langkah 1: Tentukan detail kontrol

Rincian kontrol diwarisi dari kontrol asli. Tinjau dan modifikasi detail ini sesuai kebutuhan.

Important

Kami sangat menyarankan agar Anda tidak pernah memasukkan informasi identifikasi sensitif ke dalam bidang bentuk bebas seperti detail Kontrol atau informasi Pengujian. Jika Anda membuat kontrol khusus yang berisi informasi sensitif, Anda tidak dapat membagikan kerangka kerja kustom apa pun yang berisi kontrol ini.

Untuk menentukan detail kontrol

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.

2. Di panel navigasi, pilih Control library.
3. Pilih kontrol standar atau kontrol khusus yang ingin Anda ubah, lalu pilih Buat salinan.
4. Tentukan nama baru kontrol, dan pilih Lanjutkan.
5. Di bawah Detail kontrol, sesuaikan detail kontrol sesuai kebutuhan.
6. Di bawah informasi Pengujian, buat perubahan pada instruksi sesuai kebutuhan.
7. Di bawah Tag, sesuaikan tag sesuai kebutuhan.
8. Pilih Berikutnya.

Langkah 2: Tentukan sumber bukti

Sumber bukti diwarisi dari kontrol asli. Anda dapat mengubah, menambah, atau menghapus sumber bukti sesuai kebutuhan.

Untuk menentukan sumber AWS terkelola (disarankan)

Tip

Kami menyarankan Anda memulai dengan memilih satu atau lebih kontrol umum. Jika Anda memiliki persyaratan kepatuhan yang lebih halus, Anda juga dapat memilih satu atau lebih kontrol inti yang spesifik.

Untuk menentukan sumber AWS terkelola

1. Di bawah sumber AWS terkelola, tinjau pilihan saat ini dan buat perubahan sesuai kebutuhan.
2. Untuk menambahkan kontrol umum, ikuti langkah-langkah ini:
 - a. Pilih Gunakan kontrol umum yang sesuai dengan sasaran kepatuhan Anda.
 - b. Pilih kontrol umum dari daftar dropdown.
 - c. (Opsional) Ulangi langkah 2 sesuai kebutuhan. Anda dapat menambahkan hingga lima kontrol umum.
3. Untuk menghapus kontrol umum, pilih X di sebelah nama kontrol.
4. Untuk menambahkan kontrol inti, ikuti langkah-langkah ini:
 - a. Pilih Gunakan kontrol inti yang cocok dengan pedoman preskriptif AWS .
 - b. Pilih kontrol umum dari daftar dropdown.

- c. (Opsional) Ulangi langkah 4 sesuai kebutuhan. Anda dapat menambahkan hingga 50 kontrol inti.
5. Untuk menghapus kontrol inti, pilih X di sebelah nama kontrol.
6. Untuk mengedit sumber data yang dikelola pelanggan, gunakan prosedur berikut. Jika tidak, pilih Selanjutnya.

Untuk menentukan sumber terkelola pelanggan

Untuk mengumpulkan bukti otomatis dari sumber data, Anda harus memilih tipe sumber data dan pemetaan sumber data. Detail ini dipetakan ke AWS penggunaan Anda, dan beri tahu Audit Manager tempat mengumpulkan bukti. Jika Anda ingin memberikan bukti Anda sendiri, Anda akan memilih sumber data manual sebagai gantinya.

Note

Anda bertanggung jawab untuk menjaga pemetaan sumber data yang Anda buat di langkah ini.

Untuk menentukan sumber terkelola pelanggan

1. Di bawah sumber yang dikelola Pelanggan, tinjau sumber data saat ini dan buat perubahan sesuai kebutuhan.
2. Untuk menghapus sumber data, pilih sumber data dari tabel dan pilih Hapus.
3. Untuk menambahkan sumber data baru, ikuti langkah-langkah berikut:
 - a. Pilih Gunakan sumber data untuk mengumpulkan bukti manual atau otomatis.
 - b. Pilih Tambahkan.
 - c. Pilih salah satu opsi berikut:
 - Pilih panggilan AWS API, lalu pilih panggilan API dan frekuensi pengumpulan bukti.
 - Pilih AWS CloudTrail acara, lalu pilih nama acara.
 - Pilih aturan AWS Config terkelola, lalu pilih pengidentifikasi aturan.
 - Pilih aturan AWS Config khusus, lalu pilih pengenalan aturan.
 - Pilih AWS Security Hub CSPM kontrol, lalu pilih kontrol CSPM Security Hub.
 - Pilih Sumber data manual, lalu pilih opsi:

- Unggah file — Gunakan opsi ini jika kontrol memerlukan dokumentasi sebagai bukti.
- Respons teks — Gunakan opsi ini jika kontrol memerlukan jawaban atas pertanyaan penilaian risiko.

 Tip

Untuk informasi tentang jenis sumber data otomatis dan tips pemecahan masalah, lihat [Jenis sumber data yang didukung untuk bukti otomatis](#)

Jika Anda perlu memvalidasi penyiapan sumber data Anda dengan pakar, pilih Sumber data manual untuk saat ini. Dengan begitu, Anda dapat membuat kontrol dan menambahkannya ke kerangka kerja sekarang, dan kemudian [mengedit kontrol](#) sesuai kebutuhan nanti.

- d. Di bawah Nama sumber data, berikan nama deskriptif.
 - e. (Opsional) Di bawah Detail tambahan, masukkan deskripsi sumber data dan deskripsi pemecahan masalah.
 - f. Pilih Tambahkan sumber data.
 - g. (Opsional) Untuk menambahkan sumber data lain, pilih Tambah dan ulangi langkah 3. Anda dapat menambahkan hingga 100 sumber data.
4. Setelah selesai, pilih Berikutnya.

Langkah 3: (Opsional): Tentukan rencana tindakan

Rencana aksi diwarisi dari kontrol asli. Anda dapat mengedit rencana tindakan ini sesuai kebutuhan.

 Important

Kami sangat menyarankan agar Anda tidak pernah memasukkan informasi identifikasi sensitif ke dalam bidang bentuk bebas seperti Rencana tindakan. Jika Anda membuat kontrol khusus yang berisi informasi sensitif, Anda tidak dapat membagikan kerangka kerja kustom apa pun yang berisi kontrol ini.

Untuk menentukan instruksi

1. Di bawah Judul, tinjau judul dan buat perubahan sesuai kebutuhan.

2. Di bawah Instruksi, tinjau instruksi dan buat perubahan sesuai kebutuhan.
3. Pilih Berikutnya.

Langkah 4: Tinjau dan buat kontrol

Tinjau informasi untuk kontrol. Untuk mengubah informasi untuk satu langkah, pilih Edit. Setelah selesai, pilih Buat kontrol khusus.

Langkah selanjutnya

Setelah Anda membuat kontrol kustom baru, Anda dapat menambahkannya ke kerangka kustom. Untuk mempelajari lebih lanjut, lihat [Membuat kerangka kerja khusus di AWS Audit Manager](#) atau [Mengedit kerangka kerja khusus di AWS Audit Manager](#).

Setelah menambahkan kontrol khusus ke kerangka kerja khusus, Anda dapat membuat penilaian dan mulai mengumpulkan bukti. Untuk mempelajari selengkapnya, lihat [Membuat penilaian di AWS Audit Manager](#).

Untuk meninjau kembali kontrol kustom Anda di kemudian hari, lihat [Menemukan kontrol yang tersedia di AWS Audit Manager](#). Anda dapat mengikuti langkah-langkah ini untuk menemukan kontrol kustom Anda sehingga Anda dapat melihat, mengedit, atau menghapusnya.

Sumber daya tambahan

Untuk solusi untuk mengontrol masalah di Audit Manager, lihat [Memecahkan masalah kontrol dan pengaturan kontrol](#).

Mengedit kontrol khusus di AWS Audit Manager

Anda mungkin perlu memodifikasi kontrol kustom Anda AWS Audit Manager saat persyaratan kepatuhan Anda berubah.

Halaman ini menguraikan langkah-langkah untuk mengedit detail kontrol kustom, sumber bukti, dan instruksi rencana tindakan.

Prasyarat

Prosedur berikut mengasumsikan bahwa Anda sebelumnya telah membuat kontrol khusus.

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk mengedit kontrol kustom. AWS Audit Manager Dua kebijakan yang disarankan yang memberikan izin ini adalah [AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Ikuti langkah-langkah ini untuk mengedit kontrol kustom.

Note

Saat Anda mengedit kontrol, perubahan diterapkan ke semua penilaian di mana kontrol aktif. Dalam semua penilaian tersebut, Audit Manager akan secara otomatis mulai mengumpulkan bukti sesuai dengan definisi kontrol terbaru.

Tugas

- [Langkah 1: Edit detail kontrol](#)
- [Langkah 2: Edit sumber bukti](#)
- [Langkah 3: Edit rencana tindakan](#)

Langkah 1: Edit detail kontrol

Tinjau dan edit detail kontrol sesuai kebutuhan.

Important

Kami sangat menyarankan agar Anda tidak pernah memasukkan informasi identifikasi sensitif ke dalam bidang bentuk bebas seperti detail Kontrol atau informasi Pengujian. Jika Anda membuat kontrol khusus yang berisi informasi sensitif, Anda tidak dapat membagikan kerangka kerja kustom apa pun yang berisi kontrol ini.

Untuk mengedit detail kontrol

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.

2. Di panel navigasi, pilih Control library lalu pilih Custom tab.
3. Pilih kontrol yang ingin Anda edit dan kemudian pilih Edit.
4. Di bawah Detail kontrol, edit detail kontrol sesuai kebutuhan.
5. Di bawah informasi Pengujian, edit deskripsi sesuai kebutuhan.
6. Pilih Berikutnya.

Langkah 2: Edit sumber bukti

Selanjutnya, Anda dapat mengedit, menghapus, atau menambahkan sumber bukti untuk kontrol.

Note

Saat Anda mengedit kontrol untuk memasukkan lebih banyak atau lebih sedikit sumber bukti, ini mungkin memengaruhi seberapa banyak bukti yang dikumpulkan kontrol Anda dalam penilaian mana pun yang aktif. Misalnya, jika Anda menambahkan sumber bukti, Anda mungkin memperhatikan bahwa Audit Manager melakukan lebih banyak penilaian sumber daya dan mengumpulkan lebih banyak bukti daripada sebelumnya. Jika Anda menghapus sumber bukti, kemungkinan kontrol Anda akan mengumpulkan lebih sedikit bukti untuk bergerak maju.

Untuk informasi selengkapnya tentang penilaian sumber daya dan harga, lihat [AWS Audit Manager Harga](#).

Untuk mengedit sumber AWS terkelola

Untuk mengedit sumber AWS terkelola

1. Di bawah sumber AWS terkelola, tinjau pilihan saat ini dan buat perubahan sesuai kebutuhan.
2. Untuk menambahkan kontrol umum, ikuti langkah-langkah ini:
 - a. Pilih Gunakan kontrol umum yang sesuai dengan sasaran kepatuhan Anda.
 - b. Pilih kontrol umum dari daftar dropdown.
 - c. (Opsional) Ulangi langkah 2 sesuai kebutuhan. Anda dapat menambahkan hingga lima kontrol umum.
3. Untuk menghapus kontrol umum, pilih X di sebelah nama kontrol.
4. Untuk menambahkan kontrol inti, ikuti langkah-langkah ini:

- a. Pilih Gunakan kontrol inti yang cocok dengan pedoman preskriptif AWS .
 - b. Pilih kontrol umum dari daftar dropdown.
 - c. (Opsional) Ulangi langkah 4 sesuai kebutuhan. Anda dapat menambahkan hingga 50 kontrol inti.
5. Untuk menghapus kontrol inti, pilih X di sebelah nama kontrol.
 6. Untuk menambahkan sumber data yang dikelola pelanggan, gunakan prosedur berikut. Jika tidak, pilih Selanjutnya.

Untuk mengedit sumber terkelola pelanggan

 Note

Anda bertanggung jawab untuk menjaga pemetaan sumber data yang Anda edit di langkah ini.

Untuk mengedit sumber terkelola pelanggan

1. Di bawah sumber yang dikelola Pelanggan, tinjau sumber data saat ini dan buat perubahan sesuai kebutuhan.
2. Untuk menghapus sumber data, pilih sumber data dari tabel, lalu pilih Hapus.
3. Untuk menambahkan sumber data baru, ikuti langkah-langkah berikut:
 - a. Pilih Gunakan sumber data untuk mengumpulkan bukti manual atau otomatis.
 - b. Pilih Tambahkan.
 - c. Pilih salah satu opsi berikut:
 - Pilih panggilan AWS API, lalu pilih panggilan API dan frekuensi pengumpulan bukti.
 - Pilih AWS CloudTrail acara, lalu pilih nama acara.
 - Pilih aturan AWS Config terkelola, lalu pilih pengidentifikasi aturan.
 - Pilih aturan AWS Config khusus, lalu pilih pengenalan aturan.
 - Pilih AWS Security Hub CSPM kontrol, lalu pilih kontrol CSPM Security Hub.
 - Pilih Sumber data manual, lalu pilih opsi:
 - Unggah file — Gunakan opsi ini jika kontrol memerlukan dokumentasi sebagai bukti.

- Respons teks — Gunakan opsi ini jika kontrol memerlukan jawaban atas pertanyaan penilaian risiko.

 Tip

Untuk informasi tentang jenis sumber data otomatis dan tips pemecahan masalah, lihat. [Jenis sumber data yang didukung untuk bukti otomatis](#)

Jika Anda perlu memvalidasi penyiapan sumber data Anda dengan pakar, pilih Sumber data manual untuk saat ini. Dengan begitu, Anda dapat membuat kontrol dan menambahkannya ke kerangka kerja sekarang, dan kemudian [mengedit kontrol](#) sesuai kebutuhan nanti.

- d. Di bawah Nama sumber data, berikan nama deskriptif.
 - e. (Opsional) Di bawah Detail tambahan, masukkan deskripsi sumber data dan deskripsi pemecahan masalah.
 - f. Pilih Tambahkan sumber data.
 - g. (Opsional) Untuk menambahkan sumber data lain, pilih Tambah dan ulangi langkah 3. Anda dapat menambahkan hingga 100 sumber data.
4. Setelah selesai, pilih Berikutnya.

Langkah 3: Edit rencana tindakan

Selanjutnya, tinjau dan edit rencana tindakan opsional.

 Important

Kami sangat menyarankan agar Anda tidak pernah memasukkan informasi identifikasi sensitif ke dalam bidang bentuk bebas seperti Rencana tindakan. Jika Anda membuat kontrol khusus yang berisi informasi sensitif, Anda tidak dapat membagikan kerangka kerja kustom apa pun yang berisi kontrol ini.

Untuk mengedit rencana tindakan

1. Di bawah Judul, edit judul sesuai kebutuhan.
2. Di bawah Instruksi, edit instruksi sesuai kebutuhan.

3. Pilih Berikutnya.

Langkah 4: Tinjau dan simpan

Tinjau informasi untuk kontrol. Untuk mengubah informasi untuk satu langkah, pilih Edit.

Setelah Anda selesai, pilih Simpan perubahan.

Note

Setelah Anda mengedit kontrol, perubahan akan berlaku sebagai berikut di semua penilaian aktif yang menyertakan kontrol:

- Untuk kontrol dengan panggilan AWS API sebagai tipe sumber data, perubahan berlaku pada pukul 00:00 UTC pada hari berikutnya.
- Untuk semua kontrol lainnya, perubahan segera berlaku.

Langkah selanjutnya

Ketika Anda yakin bahwa Anda tidak lagi memerlukan kontrol khusus, Anda dapat membersihkan lingkungan Audit Manager Anda dengan menghapus kontrol. Untuk petunjuk, lihat [Menghapus kontrol khusus di AWS Audit Manager](#).

Sumber daya tambahan

Untuk solusi untuk mengontrol masalah di Audit Manager, lihat [Memecahkan masalah kontrol dan pengaturan kontrol](#).

Mengubah seberapa sering kontrol mengumpulkan bukti

AWS Audit Manager dapat mengumpulkan bukti dari berbagai sumber data. Frekuensi pengumpulan bukti tergantung pada jenis sumber data yang digunakan kontrol.

Bagian berikut memberikan informasi lebih lanjut tentang frekuensi pengumpulan bukti untuk setiap jenis sumber data kontrol, dan cara mengubahnya (jika ada).

Topik

- [Poin kunci](#)

- [Snapshot konfigurasi dari panggilan AWS API](#)
- [Pemeriksaan kepatuhan dari AWS Config](#)
- [Pemeriksaan kepatuhan dari Security Hub CSPM](#)
- [Log aktivitas pengguna dari AWS CloudTrail](#)

Poin kunci

- Untuk panggilan AWS API, Audit Manager mengumpulkan bukti menggunakan panggilan API describe ke panggilan lain Layanan AWS. Anda dapat menentukan frekuensi pengumpulan bukti secara langsung di Audit Manager (hanya untuk kontrol kustom).
- Untuk AWS Config, Audit Manager melaporkan hasil pemeriksaan kepatuhan langsung dari AWS Config. Frekuensi mengikuti pemicu yang didefinisikan dalam AWS Config aturan.
- Untuk AWS Security Hub CSPM, Audit Manager melaporkan hasil pemeriksaan kepatuhan langsung dari Security Hub CSPM. Frekuensi mengikuti jadwal pemeriksaan CSPM Security Hub.
- Untuk AWS CloudTrail, Audit Manager mengumpulkan bukti secara terus menerus dari CloudTrail. Anda tidak dapat mengubah frekuensi untuk jenis bukti ini.

Snapshot konfigurasi dari panggilan AWS API

Note

Berikut ini hanya berlaku untuk kontrol khusus. Anda tidak dapat mengubah frekuensi pengumpulan bukti untuk kontrol standar.

Jika kontrol kustom menggunakan panggilan AWS API sebagai tipe sumber data, Anda dapat mengubah frekuensi pengumpulan bukti di Audit Manager dengan mengikuti langkah-langkah berikut.

Untuk mengubah frekuensi pengumpulan bukti untuk kontrol kustom dengan sumber data panggilan API

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.
2. Di panel navigasi, pilih Control library, lalu pilih Custom tab.
3. Pilih kontrol khusus yang ingin Anda edit, lalu pilih Edit.
4. Pada halaman Edit detail kontrol, pilih Berikutnya.

5. Di bawah Sumber terkelola Pelanggan, cari sumber data panggilan API yang ingin Anda perbarui.
6. Pilih sumber data dari tabel, lalu pilih Hapus.
7. Pilih Tambahkan.
8. Pilih panggilan AWS API.
9. Pilih panggilan API yang sama dengan yang Anda hapus di langkah 5, lalu pilih frekuensi pengumpulan bukti pilihan Anda.
10. Di bawah Nama sumber data, berikan nama deskriptif.
11. (Opsional) Di bawah Detail tambahan, masukkan deskripsi sumber data dan deskripsi pemecahan masalah.
12. Pilih Berikutnya.
13. Pada halaman Edit rencana tindakan, pilih Berikutnya.
14. Pada halaman Tinjau dan perbarui, tinjau informasi untuk kontrol kustom. Untuk mengubah informasi untuk satu langkah, pilih Edit.
15. Setelah Anda selesai, pilih Simpan perubahan.

Setelah Anda mengedit kontrol, perubahan akan berlaku pada pukul 00:00 UTC pada hari berikutnya di semua penilaian aktif yang menyertakan kontrol.

Pemeriksaan kepatuhan dari AWS Config

Note

Berikut ini berlaku untuk kontrol standar dan kontrol khusus yang digunakan Aturan AWS Config sebagai sumber data.

Jika kontrol digunakan AWS Config sebagai tipe sumber data, Anda tidak dapat mengubah frekuensi pengumpulan bukti secara langsung di Audit Manager. Ini karena frekuensi mengikuti pemicu yang ditentukan dalam AWS Config aturan.

Ada dua jenis pemicu untuk Aturan AWS Config:

1. Perubahan konfigurasi - AWS Config menjalankan evaluasi untuk aturan ketika jenis sumber daya tertentu dibuat, diubah, atau dihapus.

2. Berkala - AWS Config menjalankan evaluasi untuk aturan pada frekuensi yang Anda pilih (misalnya, setiap 24 jam).

Untuk mempelajari pemicu selengkapnya Aturan AWS Config, lihat [Jenis pemicu](#) di Panduan AWS Config Pengembang.

Untuk petunjuk tentang cara mengelola Aturan AWS Config, lihat [Mengelola AWS Config aturan Anda](#).

Pemeriksaan kepatuhan dari Security Hub CSPM

Note

Berikut ini berlaku untuk kontrol standar dan kontrol khusus yang menggunakan pemeriksaan CSPM Security Hub sebagai sumber data.

Jika kontrol menggunakan Security Hub CSPM sebagai tipe sumber data, Anda tidak dapat mengubah frekuensi pengumpulan bukti secara langsung di Audit Manager. Hal ini dikarenakan frekuensi mengikuti jadwal pemeriksaan CSPM Security Hub.

- Pemeriksaan berkala berjalan secara otomatis dalam waktu 12 jam setelah proses terbaru. Anda tidak dapat mengubah periodisitas.
- Pemeriksaan yang dipicu perubahan berjalan saat sumber daya terkait mengubah status. Meskipun sumber daya tidak mengubah status, pembaruan pada waktu untuk pemeriksaan yang dipicu perubahan disegarkan setiap 18 jam. Ini membantu menunjukkan bahwa kontrol masih diaktifkan. Secara umum, Security Hub CSPM menggunakan aturan yang dipicu perubahan bila memungkinkan.

Untuk mempelajari selengkapnya, lihat [Menjadwalkan untuk menjalankan pemeriksaan keamanan](#) di Panduan AWS Security Hub CSPM Pengguna.

Log aktivitas pengguna dari AWS CloudTrail

Note

Berikut ini berlaku untuk kontrol standar dan kontrol kustom yang menggunakan log aktivitas AWS CloudTrail pengguna sebagai sumber data.

Anda tidak dapat mengubah frekuensi pengumpulan bukti untuk kontrol yang menggunakan log aktivitas CloudTrail sebagai tipe sumber data. Audit Manager mengumpulkan jenis bukti ini dari CloudTrail secara terus menerus. Frekuensi terus menerus karena aktivitas pengguna dapat terjadi kapan saja sepanjang hari.

Menghapus kontrol khusus di AWS Audit Manager

Jika Anda membuat kontrol khusus dan tidak lagi membutuhkannya, Anda dapat menghapusnya dari lingkungan Audit Manager Anda. Ini memungkinkan Anda untuk membersihkan ruang kerja Anda dan fokus pada kontrol khusus yang relevan dengan tugas dan prioritas Anda saat ini.

Prasyarat

Prosedur berikut mengasumsikan bahwa Anda sebelumnya telah membuat kontrol khusus.

Pastikan identitas IAM Anda memiliki izin yang sesuai untuk menghapus kontrol khusus.

AWS Audit Manager Dua kebijakan yang disarankan yang memberikan izin ini adalah

[AWSAuditManagerAdministratorAccess](#) dan [Izinkan akses manajemen pengguna ke AWS Audit Manager](#).

Prosedur

Anda dapat menghapus kontrol kustom menggunakan konsol Audit Manager, Audit Manager API, atau AWS Command Line Interface (AWS CLI).

Important

Saat Anda menghapus kontrol kustom, tindakan ini akan menghapus kontrol dari kerangka kerja kustom atau penilaian yang saat ini terkait dengannya. Akibatnya, Audit Manager akan

berhenti mengumpulkan bukti untuk kontrol kustom tersebut di semua penilaian Anda. Ini termasuk penilaian yang sebelumnya Anda buat sebelum Anda menghapus kontrol kustom.

Audit Manager console

Untuk menghapus kontrol kustom di konsol Audit Manager

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/rumah>.
2. Di panel navigasi, pilih Control library lalu pilih tab Custom controls.
3. Pilih kontrol yang ingin Anda hapus, lalu pilih Hapus.
4. Di jendela pop-up yang muncul, pilih Hapus untuk mengonfirmasi penghapusan.

AWS CLI

Untuk menghapus kontrol kustom di AWS CLI

1. Pertama, identifikasi kontrol khusus yang ingin Anda hapus. Untuk melakukan ini, jalankan perintah [list-controls](#) dan tentukan as. `--control-type Custom`

```
aws auditmanager list-controls --control-type Custom
```

Respons mengembalikan daftar kontrol kustom. Temukan kontrol yang ingin Anda hapus, dan catat ID kontrol.

2. Selanjutnya, jalankan perintah [delete-control](#) dan gunakan `--control-id` parameter untuk menentukan kontrol yang ingin Anda hapus.

Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri.

```
aws auditmanager delete-control --control-id a1b2c3d4-5678-90ab-cdef-  
EXAMPLE11111
```

Audit Manager API

Untuk menghapus kontrol kustom menggunakan API

1. Gunakan [ListControls](#) operasi dan tentukan [ControlType](#) sebagai Custom. Dari respons, temukan kontrol yang ingin Anda hapus dan catat ID kontrol.
2. Gunakan [DeleteControl](#) operasi untuk menghapus kontrol khusus. Dalam permintaan, gunakan parameter [ControlId](#) untuk menentukan kontrol yang ingin Anda hapus.

Untuk informasi selengkapnya tentang operasi API ini, pilih salah satu tautan dalam prosedur sebelumnya untuk membaca selengkapnya di Referensi AWS Audit Manager API. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu bahasa khusus AWS SDKs.

Sumber daya tambahan

Untuk informasi tentang retensi data di Audit Manager, lihat [Penghapusan data Audit Manager](#).

Meninjau dan mengonfigurasi Anda AWS Audit Manager pengaturan

Anda dapat meninjau dan mengonfigurasi AWS Audit Manager pengaturan kapan saja untuk memastikan bahwa pengaturan tersebut memenuhi kebutuhan spesifik Anda.

Bab ini memandu Anda melalui proses mengakses, meninjau, dan menyesuaikan setelan Audit Manager Anda selangkah demi selangkah. Dengan mengikuti, Anda akan mempelajari cara mengubah pengaturan umum, pengaturan penilaian, dan pengaturan pencari bukti agar selaras dengan tujuan kepatuhan dan persyaratan bisnis Anda yang terus berkembang.

Prosedur

Untuk memulai, ikuti langkah-langkah berikut untuk melihat setelan Audit Manager Anda. Anda dapat melihat setelan Audit Manager menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API.

Untuk melihat pengaturan Anda

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Pada panel navigasi kiri, pilih Pengaturan.
3. Pilih tab yang memenuhi tujuan Anda.
 - Pengaturan umum - Pilih tab ini untuk meninjau dan memperbarui pengaturan Manajer Audit umum Anda.
 - Setelan penilaian - Pilih tab ini untuk meninjau dan memperbarui pengaturan default untuk penilaian Anda.
 - Pengaturan pencari bukti - Pilih tab ini untuk meninjau dan memperbarui pengaturan pencari bukti Anda.

Langkah selanjutnya

Untuk menyesuaikan setelan Audit Manager untuk kasus penggunaan Anda, ikuti prosedur yang diuraikan di sini.

- Pengaturan umum

- [Mengkonfigurasi pengaturan enkripsi data Anda](#)
- [Menambahkan administrator yang didelegasikan](#)
- [Mengubah administrator yang didelegasikan](#)
- [Menghapus administrator yang didelegasikan](#)
- [Menonaktifkan AWS Audit Manager](#)
- Pengaturan penilaian
 - [Mengkonfigurasi pemilik audit default Anda](#)
 - [Mengkonfigurasi tujuan laporan penilaian default](#)
 - [Mengkonfigurasi notifikasi Audit Manager](#)
- Pengaturan pencari bukti
 - [Mengaktifkan pencari bukti](#)
 - [Mengkonfirmasi status pencari bukti](#)
 - [Mengkonfigurasi tujuan ekspor default Anda untuk pencari bukti](#)
 - [Menonaktifkan pencari bukti](#)

Mengkonfigurasi pengaturan enkripsi data Anda

Anda dapat memilih bagaimana Anda mengenkripsi data Anda AWS Audit Manager. Audit Manager secara otomatis membuat unik Kunci yang dikelola AWS untuk penyimpanan data yang aman. Secara default, data Audit Manager Anda dienkripsi dengan kunci KMS ini. Namun, jika Anda ingin menyesuaikan pengaturan enkripsi data, Anda dapat menentukan kunci yang dikelola pelanggan enkripsi simetris Anda sendiri. Menggunakan kunci KMS Anda sendiri memberi Anda lebih banyak fleksibilitas, termasuk kemampuan untuk membuat, memutar, dan menonaktifkan tombol.

Menggunakan kunci yang dikelola pelanggan juga memberikan lapisan perlindungan tambahan untuk laporan penilaian Anda. Audit Manager mengenkripsi laporan dengan kunci KMS Anda sebelum menulisnya ke Amazon S3. Isi laporan tidak dapat dibaca tanpa akses ke kunci Anda. Ini melindungi data Anda bahkan jika bucket S3 tujuan laporan penilaian Anda dikompromikan.

Prasyarat

Jika Anda memberikan kunci yang dikelola pelanggan, kunci tersebut harus Wilayah AWS sama dengan penilaian Anda agar dapat menghasilkan laporan penilaian dan mengeksport hasil pencarian pencari bukti dengan sukses.

Prosedur

Anda dapat memperbarui setelan enkripsi data menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API.

Note

Saat Anda mengubah setelan enkripsi data Audit Manager, perubahan ini berlaku untuk penilaian baru yang Anda buat. Ini termasuk laporan penilaian dan ekspor pencari bukti yang Anda buat dari penilaian baru Anda.

Perubahan tidak berlaku untuk penilaian yang sudah ada yang Anda buat sebelum mengubah setelan enkripsi. Ini termasuk laporan penilaian baru dan ekspor CSV yang Anda buat dari penilaian yang ada, selain laporan penilaian yang ada dan ekspor CSV. Penilaian yang ada—dan semua laporan penilaian serta ekspor CSV—terus menggunakan kunci KMS lama. Jika identitas IAM yang menghasilkan laporan penilaian tidak dapat menggunakan kunci KMS lama, berikan izin di tingkat kebijakan utama.

Audit Manager console

Untuk memperbarui setelan enkripsi data Anda di konsol Audit Manager

1. Dari tab Pengaturan Umum, buka bagian Enkripsi data.
2. Untuk menggunakan kunci KMS default yang disediakan oleh Audit Manager, kosongkan kotak centang Kustomisasi pengaturan enkripsi (lanjutan).
3. Untuk menggunakan kunci yang dikelola pelanggan, pilih kotak centang Kustomisasi pengaturan enkripsi (lanjutan). Anda kemudian dapat memilih kunci KMS yang ada, atau membuat yang baru.

AWS CLI

Untuk memperbarui pengaturan enkripsi data Anda di AWS CLI

Jalankan [perintah](#) `update-settings` dan gunakan `--kms-key` parameter untuk menentukan kunci yang dikelola pelanggan Anda sendiri.

Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri.

```
aws auditmanager update-settings --kms-key arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Audit Manager API

Untuk memperbarui setelan enkripsi data menggunakan API

Panggil [UpdateSettings](#) operasi dan gunakan [parameter K](#) MSkey untuk menentukan kunci yang dikelola pelanggan Anda sendiri.

Untuk informasi selengkapnya, pilih tautan sebelumnya untuk membaca lebih lanjut di Referensi API Manajer Audit. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasa AWS .

Sumber daya tambahan

- Untuk petunjuk tentang cara membuat kunci, lihat [Membuat kunci](#) di Panduan AWS Key Management Service Pengguna.
- Untuk petunjuk tentang cara memberikan izin di tingkat kebijakan utama, lihat Mengiz [inkan pengguna di akun lain menggunakan kunci KMS](#) di Panduan Peng AWS Key Management Service embang.

Menambahkan administrator yang didelegasikan

Jika Anda menggunakan AWS Organizations dan ingin mengaktifkan dukungan multi-akun untuk AWS Audit Manager, Anda dapat menetapkan akun anggota di organisasi Anda sebagai administrator yang didelegasikan untuk Manajer Audit.

Jika Anda ingin menggunakan Audit Manager di lebih dari satu Wilayah AWS, Anda harus menetapkan akun administrator yang didelegasikan secara terpisah di setiap Wilayah. Di setelan Audit Manager, Anda harus menggunakan akun administrator yang didelegasikan yang sama di semua Wilayah.

Prasyarat

Perhatikan faktor-faktor berikut yang menentukan bagaimana administrator yang didelegasikan beroperasi di Audit Manager:

- Akun Anda harus menjadi bagian dari organisasi.
- Sebelum menunjuk administrator yang didelegasikan, Anda harus [mengaktifkan semua fitur di organisasi Anda](#). Anda juga harus [mengonfigurasi setelan CSPM Security Hub organisasi Anda](#). Dengan cara ini, Audit Manager dapat mengumpulkan bukti CSPM Security Hub dari akun anggota Anda.
- Akun administrator yang didelegasikan harus memiliki akses pada kunci KMS yang Anda berikan saat menyiapkan Audit Manager.
- Anda tidak dapat menggunakan akun AWS Organizations manajemen sebagai administrator yang didelegasikan di Audit Manager.

Prosedur

Anda dapat menambahkan administrator yang didelegasikan menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau API Audit Manager.

Note

Setelah menambahkan administrator yang didelegasikan di setelan Audit Manager, akun manajemen Anda tidak dapat lagi membuat penilaian tambahan di Audit Manager. Selain itu, pengumpulan bukti berhenti untuk penilaian yang ada yang dibuat oleh akun manajemen. Manajer Audit mengumpulkan dan melampirkan bukti ke akun administrator yang didelegasikan, yang merupakan akun utama untuk mengelola penilaian organisasi Anda.

Audit Manager console

Untuk menambahkan administrator yang didelegasikan di konsol Audit Manager

1. Dari tab Pengaturan umum, buka bagian Administrator yang didelegasikan.
2. Di bawah ID akun administrator yang didelegasikan, masukkan ID akun administrator yang didelegasikan.
3. Pilih Delegasikan.

AWS CLI

Untuk menambahkan administrator yang didelegasikan di AWS CLI

Jalankan [perintah](#) `register-organization-admin-account` dan gunakan `--admin-account-id` parameter untuk menentukan ID akun dari administrator yang didelegasikan.

Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri.

```
aws auditmanager register-organization-admin-account --admin-account-id 111122223333
```

Audit Manager API

Untuk menambahkan administrator yang didelegasikan menggunakan API

Panggil [RegisterOrganizationAdminAccount](#) operasi dan gunakan AccountId [parameter](#) admin untuk menentukan ID akun dari administrator yang didelegasikan.

Untuk informasi selengkapnya, pilih tautan sebelumnya untuk membaca lebih lanjut di Referensi API Manajer Audit. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasa AWS .

Langkah selanjutnya

Untuk mengubah akun administrator yang didelegasikan, lihat [Mengubah administrator yang didelegasikan](#).

Untuk menghapus akun administrator yang didelegasikan, lihat [Menghapus administrator yang didelegasikan](#).

Sumber daya tambahan

- [Menciptakan dan mengelola organisasi](#)
- [Pemecahan masalah administrator yang didelegasikan dan AWS Organizations masalah](#)

Mengubah administrator yang didelegasikan

Mengubah administrator yang didelegasikan AWS Audit Manager adalah proses dua langkah. Pertama, Anda perlu menghapus akun administrator yang didelegasikan saat ini. Kemudian, Anda dapat menambahkan akun baru sebagai administrator yang didelegasikan.

Ikuti langkah-langkah di halaman ini untuk mengubah administrator yang didelegasikan.

Daftar Isi

- [Prasyarat](#)
 - [Sebelum Anda menghapus akun saat ini](#)
 - [Sebelum Anda menambahkan akun baru](#)
- [Prosedur](#)
- [Langkah selanjutnya](#)
- [Sumber daya tambahan](#)

Prasyarat

Sebelum Anda menghapus akun saat ini

Sebelum Anda menghapus akun administrator yang didelegasikan saat ini, ingatlah pertimbangan berikut:

- Tugas pembersihan pencari bukti - Jika administrator yang didelegasikan saat ini (akun A) mengaktifkan pencari bukti, Anda harus melakukan tugas pembersihan sebelum menetapkan akun B sebagai administrator yang didelegasikan baru.

Sebelum menggunakan akun manajemen untuk menghapus akun A, pastikan akun A masuk ke Manajer Audit dan menonaktifkan pencari bukti. Menonaktifkan pencari bukti secara otomatis menghapus penyimpanan data peristiwa yang dibuat di akun saat pencari bukti diaktifkan.

Jika tugas ini tidak selesai, penyimpanan data peristiwa tetap berada di akun A. Dalam hal ini, sebaiknya administrator delegasi asli menggunakan CloudTrail Lake untuk [menghapus penyimpanan data peristiwa secara manual](#).

Tugas pembersihan ini diperlukan untuk memastikan bahwa Anda tidak berakhir dengan beberapa penyimpanan data peristiwa. Audit Manager mengabaikan penyimpanan data peristiwa yang tidak digunakan setelah Anda menghapus atau mengubah akun administrator yang didelegasikan. Namun, jika Anda tidak menghapus penyimpanan data peristiwa yang tidak digunakan, penyimpanan data peristiwa akan terus mengeluarkan biaya penyimpanan dari CloudTrail Lake.

- Penghapusan data - Saat Anda menghapus akun administrator yang didelegasikan untuk Audit Manager, data untuk akun tersebut tidak dihapus. Jika Anda ingin menghapus data sumber daya untuk akun administrator yang didelegasikan, Anda harus melakukan tugas tersebut secara

terpisah sebelum menghapus akun. Entah, Anda dapat melakukan ini di konsol Audit Manager. Atau, Anda dapat menggunakan salah satu operasi penghapusan API yang disediakan oleh Audit Manager. Untuk daftar operasi penghapusan yang tersedia, lihat Pengh [apusan data Manajer Audit](#).

Saat ini, Audit Manager tidak menyediakan opsi untuk menghapus bukti untuk administrator yang didelegasikan tertentu. Sebaliknya, ketika akun manajemen Anda membatalkan pendaftaran Manajer Audit, kami melakukan pembersihan untuk akun administrator yang didelegasikan saat ini pada saat deregistrasi.

Sebelum Anda menambahkan akun baru

Sebelum menambahkan akun administrator baru yang didelegasikan, ingatlah pertimbangan berikut:

- Akun baru harus menjadi bagian dari organisasi.
- Sebelum menunjuk administrator baru yang didelegasikan, Anda harus [mengaktifkan semua fitur di organisasi Anda](#). Anda juga harus [mengonfigurasi setelan CSPM Security Hub organisasi Anda](#). Dengan cara ini, Audit Manager dapat mengumpulkan bukti CSPM Security Hub dari akun anggota Anda.
- Akun administrator yang didelegasikan harus memiliki akses pada kunci KMS yang Anda berikan saat menyiapkan Audit Manager.
- Anda tidak dapat menggunakan akun AWS Organizations manajemen sebagai administrator yang didelegasikan di Audit Manager.

Prosedur

Anda dapat mengubah administrator yang didelegasikan menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau API Audit Manager.

Warning

Saat Anda mengubah administrator yang didelegasikan, Anda tetap memiliki akses ke bukti yang sebelumnya Anda kumpulkan di bawah akun administrator lama yang didelegasikan. Namun, Audit Manager berhenti mengumpulkan dan melampirkan bukti ke akun administrator lama yang didelegasikan.

Audit Manager console

Untuk mengubah administrator yang didelegasikan saat ini di konsol Audit Manager

1. (Opsional) Jika administrator yang didelegasikan saat ini (akun A) mengaktifkan pencari bukti, lakukan tugas pembersihan berikut:

- Sebelum menetapkan akun B sebagai administrator baru yang didelegasikan, pastikan akun A masuk ke Manajer Audit dan menonaktifkan pencari bukti.

Menonaktifkan pencari bukti secara otomatis menghapus penyimpanan data peristiwa yang dibuat saat akun A mengaktifkan pencari bukti. Jika Anda tidak menyelesaikan langkah ini, maka akun A harus pergi ke CloudTrail Lake dan [menghapus penyimpanan data peristiwa secara manual](#). Jika tidak, penyimpanan data peristiwa tetap berada di akun A dan terus dikenakan biaya penyimpanan CloudTrail Danau.

2. Dari tab Pengaturan umum, buka bagian Administrator yang didelegasikan dan pilih Hapus.
3. Di jendela pop-up yang muncul, pilih Hapus untuk mengonfirmasi.
4. Di bawah ID akun administrator yang didelegasikan, masukkan ID akun administrator yang baru didelegasikan.
5. Pilih Delegasikan.

AWS CLI

Untuk mengubah administrator yang didelegasikan saat ini di AWS CLI

Pertama, jalankan [perintah](#) `deregister-organization-admin-account` menggunakan `--admin-account-id` parameter untuk menentukan ID akun dari administrator yang didelegasikan saat ini.

Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri.

```
aws auditmanager deregister-organization-admin-account --admin-account-id 111122223333
```

Kemudian, jalankan [perintah](#) `register-organization-admin-account` menggunakan `--admin-account-id` parameter untuk menentukan ID akun dari administrator yang didelegasikan baru.

Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri.


```
aws auditmanager register-organization-admin-account --admin-account-id 444455556666
```

Audit Manager API

Untuk mengubah administrator yang didelegasikan saat ini menggunakan API

Pertama, panggil [DeregisterOrganizationAdminAccount](#) operasi dan gunakan AccountId [parameter](#) admin untuk menentukan ID akun dari administrator yang didelegasikan saat ini.

Kemudian, panggil [RegisterOrganizationAdminAccount](#) operasi dan gunakan AccountId [parameter](#) admin untuk menentukan ID akun dari administrator yang didelegasikan baru.

Untuk informasi selengkapnya, pilih tautan sebelumnya untuk membaca lebih lanjut di Referensi API Manajer Audit. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasa AWS .

Langkah selanjutnya

Untuk menghapus akun administrator yang didelegasikan, lihat [Menghapus administrator yang didelegasikan](#).

Sumber daya tambahan

- [Menciptakan dan mengelola organisasi](#)
- [Pemecahan masalah administrator yang didelegasikan dan AWS Organizations masalah](#)

Menghapus administrator yang didelegasikan

Menghapus akun administrator yang didelegasikan menghentikan pengumpulan bukti lebih lanjut untuk akun tersebut, tetapi Anda tetap mempertahankan akses ke bukti yang dikumpulkan sebelumnya.

Jika Anda perlu menghapus akun administrator yang didelegasikan untuk Audit Manager, Anda dapat mengikuti langkah-langkah yang diperlukan di halaman ini. Ikuti prasyarat dan prosedur dengan hati-hati, karena melibatkan pembersihan sumber daya untuk menghindari biaya penyimpanan yang tidak perlu.

Prasyarat

Sebelum Anda menghapus akun administrator yang didelegasikan dari Audit Manager, ingatlah pertimbangan berikut:

Tugas pembersihan pencari bukti

Jika administrator yang didelegasikan saat ini mengaktifkan pencari bukti, Anda perlu melakukan tugas pembersihan.

Sebelum Anda menggunakan akun manajemen untuk menghapus administrator yang didelegasikan saat ini, pastikan akun administrator yang didelegasikan saat ini masuk ke Manajer Audit dan menonaktifkan pencari bukti. Menonaktifkan pencari bukti secara otomatis menghapus penyimpanan data peristiwa yang dibuat di akun saat pencari bukti diaktifkan.

Jika tugas ini tidak selesai, penyimpanan data peristiwa tetap ada di akun mereka. Dalam hal ini, sebaiknya administrator delegasi asli menggunakan CloudTrail Lake untuk [menghapus penyimpanan data peristiwa secara manual](#).

Tugas pembersihan ini diperlukan untuk memastikan bahwa Anda tidak berakhir dengan beberapa penyimpanan data peristiwa. Audit Manager mengabaikan penyimpanan data peristiwa yang tidak digunakan setelah Anda menghapus atau mengubah akun administrator yang didelegasikan. Namun, jika Anda tidak menghapus penyimpanan data peristiwa yang tidak digunakan, penyimpanan data peristiwa akan terus mengeluarkan biaya penyimpanan dari CloudTrail Lake.

Penghapusan data

Saat Anda menghapus akun administrator yang didelegasikan untuk Audit Manager, data untuk akun tersebut tidak dihapus. Jika Anda ingin menghapus data sumber daya untuk akun administrator yang didelegasikan, Anda harus melakukan tugas tersebut secara terpisah sebelum menghapus akun. Entah, Anda dapat melakukan ini di konsol Audit Manager. Atau, Anda dapat menggunakan salah satu operasi penghapusan API yang disediakan oleh Audit Manager. Untuk daftar operasi penghapusan yang tersedia, lihat Pengh [apusan data Manajer Audit](#).

Saat ini, Audit Manager tidak menyediakan opsi untuk menghapus bukti untuk administrator yang didelegasikan tertentu. Sebaliknya, ketika akun manajemen Anda membatalkan pendaftaran Manajer Audit, kami melakukan pembersihan untuk akun administrator yang didelegasikan saat ini pada saat deregistrasi.

Prosedur

Anda dapat menghapus administrator yang didelegasikan menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau API Audit Manager.

Warning

Saat menghapus administrator yang didelegasikan, Anda tetap memiliki akses ke bukti yang sebelumnya Anda kumpulkan di bawah akun administrator yang didelegasikan tersebut. Namun, Audit Manager berhenti mengumpulkan dan melampirkan bukti ke akun administrator lama yang didelegasikan.

Audit Manager console

Untuk menghapus administrator yang didelegasikan saat ini di konsol Audit Manager

1. (Opsional) Jika administrator yang didelegasikan saat ini mengaktifkan pencari bukti, lakukan tugas pembersihan berikut:
 - Pastikan akun administrator yang didelegasikan saat ini masuk ke Audit Manager dan menonaktifkan pencari bukti.

Menonaktifkan pencari bukti secara otomatis menghapus penyimpanan data peristiwa yang dibuat di akun mereka saat mereka mengaktifkan pencari bukti. Jika langkah ini tidak selesai, akun administrator yang didelegasikan harus menggunakan CloudTrail Lake untuk [menghapus penyimpanan data peristiwa secara manual](#). Jika tidak, penyimpanan data acara tetap ada di akun mereka dan terus dikenakan biaya penyimpanan CloudTrail Danau.
2. Dari tab Pengaturan umum, buka bagian Administrator yang didelegasikan dan pilih Hapus.
3. Di jendela pop-up yang muncul, pilih Hapus untuk mengonfirmasi.

AWS CLI

Menonaktifkan pencari bukti secara otomatis menghapus penyimpanan data peristiwa yang dibuat di akun mereka saat mereka mengaktifkan pencari bukti. Jika langkah ini tidak selesai, akun administrator yang didelegasikan harus menggunakan CloudTrail Lake untuk [menghapus](#)

[penyimpanan data peristiwa secara manual](#). Jika tidak, penyimpanan data acara tetap ada di akun mereka dan terus dikenakan biaya penyimpanan CloudTrail Danau.

Untuk menghapus administrator yang didelegasikan saat ini di AWS CLI

Jalankan [perintah](#) `deregister-organization-admin-account` dan gunakan `--admin-account-id` parameter untuk menentukan ID akun dari administrator yang didelegasikan.

Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri.

```
aws auditmanager deregister-organization-admin-account --admin-account-id 111122223333
```

Audit Manager API

Untuk menghapus administrator yang didelegasikan saat ini menggunakan API

Panggil [DeregisterOrganizationAdminAccount](#) operasi dan gunakan AccountId [parameter](#) admin untuk menentukan ID akun dari administrator yang didelegasikan.

Untuk informasi selengkapnya, pilih tautan sebelumnya untuk membaca lebih lanjut di Referensi API Manajer Audit. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasa AWS .

Sumber daya tambahan

- [Pemecahan masalah administrator yang didelegasikan dan AWS Organizations masalah](#)

Mengkonfigurasi pemilik audit default Anda

Anda dapat menggunakan pengaturan ini untuk menentukan default yang [audit owner](#) memiliki akses utama ke penilaian Anda di Manajer Audit.

Prosedur

Anda dapat memperbarui setelan ini menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API.

Audit Manager console

Anda dapat memilih dari yang Akun AWS tercantum dalam tabel, atau menggunakan bilah pencarian untuk mencari yang lain Akun AWS.

Untuk memperbarui pemilik audit default Anda di konsol Audit Manager

1. Dari tab Pengaturan penilaian, buka bagian Pemilik audit default dan pilih Edit.
2. Untuk menambahkan pemilik audit default, pilih kotak centang di samping nama akun di bawah Pemilik audit.
3. Untuk menghapus pemilik audit default, kosongkan kotak centang di samping nama akun di bawah Pemilik audit.
4. Setelah selesai, pilih Simpan.

AWS CLI

Untuk memperbarui pemilik audit default Anda di AWS CLI

Jalan [kan](#) perintah `update-settings` dan gunakan `--default-process-owners` parameter untuk menentukan pemilik audit.

Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri. Perhatikan bahwa hanya `roleType` bisa `PROCESS_OWNER`.

```
aws auditmanager update-settings --default-process-owners
roleType=PROCESS_OWNER,roleArn=arn:aws:iam::111122223333:role/Administrator
```

Audit Manager API

Untuk memperbarui pemilik audit default Anda menggunakan API

Panggil [UpdateSettings](#) operasi dan gunakan `ProcessOwners` [parameter](#) default untuk menentukan pemilik audit default. Perhatikan bahwa hanya `roleType` bisa `PROCESS_OWNER`.

Sumber daya tambahan

- Untuk informasi selengkapnya tentang pemilik [audit](#), lihat [Pemilik audit](#) di bagian Konsep dan terminologi panduan ini.

Mengkonfigurasi tujuan laporan penilaian default

Saat Anda membuat laporan penilaian, Audit Manager menerbitkan laporan ke bucket S3 pilihan Anda. Bucket S3 ini disebut sebagai [assessment report destination](#). Anda dapat memilih bucket S3 tempat Audit Manager menyimpan laporan penilaian Anda.

Prasyarat

Kiat konfigurasi untuk tujuan laporan penilaian Anda

Untuk memastikan keberhasilan pembuatan laporan penilaian Anda, sebaiknya gunakan konfigurasi berikut untuk tujuan laporan penilaian Anda.

Same-Region ember

Sebaiknya gunakan bucket S3 yang Wilayah AWS sama dengan penilaian Anda. Saat Anda menggunakan bucket dan penilaian wilayah yang sama, laporan penilaian Anda dapat mencakup hingga 22.000 item bukti. Sebaliknya, ketika Anda menggunakan bucket dan penilaian lintas wilayah, hanya 3.500 item bukti yang dapat dimasukkan.

Wilayah AWS

K Wilayah AWS unci yang dikelola pelanggan Anda (jika Anda menyediakannya) harus sesuai dengan Wilayah penilaian Anda dan bucket S3 tujuan laporan penilaian Anda. Untuk petunjuk tentang cara mengubah kunci KMS, lihat [Mengkonfigurasi pengaturan enkripsi data Anda](#). Untuk daftar Wilayah Manajer Audit yang didukung, lihat [AWS Audit Manager titik akhir dan kuota](#) di Referensi Umum Amazon Web Services.

Enkripsi bucket S3

Jika tujuan laporan penilaian Anda memiliki kebijakan bucket yang memerlukan penggunaan enkripsi sisi server (SSE) [SSE-KMS](#), maka kunci KMS yang digunakan dalam kebijakan bucket tersebut harus sesuai dengan kunci KMS yang Anda konfigurasi di setelan enkripsi data Audit Manager Anda. Jika Anda belum mengonfigurasi kunci KMS di setelan Audit Manager, dan kebijakan bucket tujuan laporan penilaian Anda memerlukan SSE, pastikan kebijakan bucket memungkinkan [SSE-S3](#). Untuk petunjuk tentang cara mengonfigurasi kunci KMS yang digunakan untuk enkripsi data, lihat [Mengkonfigurasi pengaturan enkripsi data Anda](#).

Cross-account Bucket S3

Menggunakan bucket S3 lintas akun sebagai tujuan laporan penilaian Anda tidak didukung di konsol Audit Manager. Anda dapat menentukan bucket lintas akun sebagai tujuan laporan penilaian Anda dengan menggunakan AWS CLI atau salah satu AWS SDK, tetapi untuk kesederhanaan, kami menyarankan Anda untuk tidak melakukan ini.

Tip

Untuk keamanan dan kinerja yang optimal, sebaiknya gunakan bucket S3 di AWS akun dan wilayah yang sama dengan penilaian Anda.

Jika Anda memilih untuk menggunakan bucket S3 lintas akun sebagai tujuan laporan penilaian Anda, pertimbangkan hal-hal berikut.

- Secara default, objek S3 — seperti laporan penilaian — dimiliki oleh yang mengunggah objek. Akun AWS Anda dapat menggunakan [set](#) elan Kepemilikan Objek S3 untuk mengubah perilaku default ini sehingga setiap objek baru yang ditulis oleh akun dengan daftar bucket-owner-full-control kontrol akses tersimpan (ACL) secara otomatis menjadi milik pemilik bucket.

Meskipun ini bukan persyaratan, kami sarankan Anda membuat perubahan berikut pada pengaturan bucket lintas akun Anda. Membuat perubahan ini memastikan bahwa pemilik bucket memiliki kontrol penuh atas laporan penilaian yang Anda publikasikan ke bucket mereka.

- [Tetapkan kepemilikan objek bucket S3](#) ke bucket owner yang lebih disukai, bukan penulis objek default
- [Tambahkan kebijakan bucket](#) untuk memastikan bahwa objek yang diunggah ke bucket tersebut memiliki bucket-owner-full-control ACL
- Untuk mengizinkan Audit Manager menerbitkan laporan dalam bucket S3 lintas akun, Anda harus menambahkan kebijakan bucket S3 berikut ke tujuan laporan penilaian Anda. Ganti *placeholder text* dengan informasi Anda sendiri. PrincipalElemen dalam kebijakan ini adalah pengguna atau peran yang memiliki penilaian dan membuat laporan penilaian. Menentukan bucket S3 lintas akun tempat laporan diterbitkan.

JSON

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "Allow cross account assessment report publishing",
    "Effect": "Allow",
    "Principal": {
      "AWS":
"arn:aws:iam::111122223333:user/AssessmentOwnerUserName"
    },
    "Action": [
      "s3:ListBucket",
      "s3:PutObject",
      "s3:GetObject",
      "s3:GetBucketLocation",
      "s3:PutObjectAcl",
      "s3:DeleteObject"
    ],
    "Resource": [
      "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
      "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
    ]
  }
]
}

```

Praktik terbaik keamanan untuk tujuan laporan penilaian Anda

Audit Manager menerbitkan laporan penilaian Anda ke bucket Amazon S3 yang Anda tentukan sebagai tujuan laporan penilaian Anda. Di bawah Model AWS Tanggung Jawab Bersama, Anda bertanggung jawab untuk mengonfirmasi bahwa orang ter Akun AWS percaya memiliki bucket ini. Untuk informasi selengkapnya tentang tanggung jawab keamanan Anda, lihat Model [AWS Tanggung Jawab Bersama](#) di AWS situs web.

Untuk melindungi laporan penilaian Anda, kami sarankan Anda menerapkan satu atau beberapa kontrol berikut.

Batasi tindakan S3 ke akun tepercaya dengan menggunakan kunci **s3:ResourceAccount** kondisi

Tambahkan **s3:ResourceAccount** kondisi ke kebijakan IAM yang dilampirkan ke identitas yang digunakan Manajer Audit untuk menerbitkan laporan penilaian. Kondisi ini mencegah identitas

menulis ke bucket yang dimiliki oleh akun selain yang Anda tentukan. Kondisi ini berlaku terlepas dari kebijakan akses bucket itu sendiri.

Untuk informasi selengkapnya, lihat [Membatasi akses ke bucket Amazon S3 yang dimiliki oleh akun AWS tertentu](#).

Batasi tindakan S3 ke organisasi Anda dengan menggunakan SCP

Jika Anda menggunakan, buat kebijakan kontrol layanan (SCP) yang menolak tindakan S3 pada sumber daya di luar organisasi Anda. Kebijakan contoh berikut menolak semua tindakan S3 ke sumber daya di luar organisasi Anda. Kondisi memeriksa apakah sesuai `aws:ResourceOrgID` dengan ID organisasi Anda.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyS3ActionsOutsideOrganization",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:ResourceOrgID": "o-xxxxxxxxxx"
        }
      }
    }
  ]
}
```

Ganti `o-xxxxxxxxxx` dengan ID organisasi Anda. Untuk informasi selengkapnya, lihat [aws:ResourceOrg ID](#) di Panduan Pengguna IAM.

Menggunakan kunci KMS yang dikelola pelanggan untuk enkripsi data

Saat Anda mengonfigurasi Audit Manager untuk menggunakan kunci yang dikelola pelanggan untuk enkripsi data, Audit Manager mengenkripsi laporan penilaian sebelum menulisnya ke Amazon S3. Jika laporan dipublikasikan ke bucket yang dimiliki oleh pihak yang tidak berwenang, konten laporan tetap dienkripsi. Konten tidak dapat dibaca tanpa akses ke kunci KMS Anda. Untuk petunjuk, lihat [Mengkonfigurasi pengaturan enkripsi data Anda](#).

Menggunakan bucket S3 di namespace regional akun Anda

Bucket S3 yang dibuat di namespace regional akun Anda menyertakan Akun AWS ID Anda dan Wilayah AWS nama bucket. Tidak ada akun lain yang dapat membuat bucket ini atau mengklaim nama bucket. Untuk informasi selengkapnya, lihat [Account-level ruang nama bucket](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Prosedur

Anda dapat memperbarui setelan ini menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API.

Audit Manager console

Untuk memperbarui tujuan laporan penilaian default Anda di konsol Audit Manager

1. Dari tab Pengaturan penilaian, buka bagian tujuan laporan penilaian.
2. Untuk menggunakan bucket S3 yang ada, pilih nama bucket dari menu dropdown.
3. Untuk membuat bucket S3 baru, pilih Buat bucket baru.
4. Setelah selesai, pilih Simpan.

AWS CLI

Untuk memperbarui tujuan laporan penilaian default Anda di AWS CLI

Jalan [kan](#) perintah `update-settings` dan gunakan `--default-assessment-reports-destination` parameter untuk menentukan bucket S3.

Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri:

```
aws auditmanager update-settings --default-assessment-reports-destination
destinationType=S3,destination=s3://amzn-s3-demo-destination-bucket
```

Audit Manager API

Untuk memperbarui tujuan laporan penilaian default Anda menggunakan API

Panggil [UpdateSettings](#) operasi dan gunakan `AssessmentReportsDestination` [parameter](#) default untuk menentukan bucket S3.

Sumber daya tambahan

- [Membuat bucket](#)
- [Laporan penilaian](#)

Mengkonfigurasi notifikasi Audit Manager

Anda dapat mengonfigurasi Audit Manager untuk mengirim pemberitahuan ke topik Amazon SNS pilihan Anda. Jika Anda berlangganan topik SNS tersebut, Anda akan menerima pemberitahuan secara langsung setiap kali masuk ke Audit Manager.

Ikuti langkah-langkah di halaman ini untuk mempelajari cara melihat dan memperbarui pengaturan notifikasi agar sesuai dengan preferensi Anda. Anda dapat menggunakan topik SNS standar atau topik SNS FIFO (first-in-first-out). Meskipun Audit Manager mendukung pengiriman notifikasi ke topik FIFO, urutan pengiriman pesan tidak dijamin.

Prasyarat

Jika Anda ingin menggunakan topik Amazon SNS yang tidak Anda miliki, Anda harus mengonfigurasi kebijakan AWS Identity and Access Management (IAM) untuk ini. Lebih khusus lagi, Anda harus mengonfigurasinya untuk mengizinkan penerbitan dari Nama Sumber Daya Amazon (ARN) topik. Untuk contoh kebijakan yang dapat Anda gunakan, lihat [Contoh 1 \(Izin untuk topik SNS\)](#).

Prosedur

Anda dapat memperbarui setelan ini menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API.

Audit Manager console

Untuk memperbarui setelan notifikasi di konsol Audit Manager

1. Dari tab Pengaturan Penilaian, buka bagian Pemberitahuan.
2. Untuk menggunakan topik SNS yang ada, pilih nama topik dari menu dropdown.
3. Untuk membuat topik SNS baru, pilih Buat topik baru.
4. Setelah selesai, pilih Simpan.

AWS CLI

Untuk memperbarui pengaturan notifikasi Anda di AWS CLI

Jalankan [perintah](#) `update-settings` dan gunakan `--sns-topic` parameter untuk menentukan topik SNS.

Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri:

```
aws auditmanager update-settings --sns-topic arn:aws:sns:us-east-1:111122223333:my-assessment-topic
```

Audit Manager API

Untuk memperbarui setelan notifikasi menggunakan API

Panggil [UpdateSettings](#) operasi dan gunakan [parameter](#) `SNSTopic` untuk menentukan topik SNS.

Sumber daya tambahan

- Untuk petunjuk tentang cara membuat topik Amazon SNS, lihat [Membuat topik Amazon SNS](#) di Panduan Pengguna Amazon SNS.
- Untuk contoh kebijakan yang dapat Anda gunakan untuk mengizinkan Audit Manager mengirim pemberitahuan ke topik Amazon SNS, lihat [Contoh 1 \(Izin untuk topik SNS\)](#)
- Untuk mempelajari selengkapnya tentang daftar tindakan yang memanggil notifikasi di Audit Manager, lihat [Pemberitahuan di AWS Audit Manager](#).
- Untuk solusi masalah notifikasi di Audit Manager, lihat [Memecahkan masalah pemberitahuan](#).

Mengaktifkan pencari bukti

Anda dapat mengaktifkan fitur pencari bukti di Audit Manager untuk mencari bukti di Akun AWS. Jika Anda adalah administrator yang didelegasikan untuk Manajer Audit, Anda dapat mencari bukti untuk semua akun anggota di organisasi Anda.

Ikuti langkah-langkah ini untuk mempelajari cara mengaktifkan pencari bukti. Perhatikan prasyarat, karena Anda memerlukan izin khusus untuk membuat dan mengelola penyimpanan data peristiwa di CloudTrail Lake untuk fungsi ini.

Prasyarat

Izin yang diperlukan untuk mengaktifkan pencari bukti

Untuk mengaktifkan pencari bukti, Anda memerlukan izin untuk membuat dan mengelola penyimpanan data peristiwa di CloudTrail Lake. Untuk menggunakan fitur ini, Anda memerlukan izin untuk melakukan kueri CloudTrail Lake. Untuk contoh kebijakan izin yang dapat Anda gunakan, lihat [Contoh 3 \(Izin untuk mengaktifkan pencari bukti\)](#).

Jika Anda memerlukan bantuan dengan izin, hubungi AWS administrator Anda. Jika Anda seorang AWS administrator, Anda dapat menyalin pernyataan izin yang diperlukan dan [melampirkannya ke kebijakan](#) IAM.

Prosedur

Meminta untuk mengaktifkan pencari bukti

Anda dapat menyelesaikan tugas ini menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API.

Note

Anda harus mengaktifkan pencari bukti di setiap Wilayah AWS tempat Anda ingin mencari bukti.

Audit Manager console

Untuk meminta untuk mengaktifkan pencari bukti di konsol Audit Manager

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Dari tab pengaturan pencari bukti, buka bagian pencari bukti.
3. Pilih Kebijakan izin yang diperlukan, lalu Lihat izin CloudTrail Lake untuk melihat izin pencari bukti yang diperlukan. Jika Anda belum memiliki izin ini, Anda dapat menyalin pernyataan kebijakan ini dan [melampirkannya ke kebijakan](#) IAM.
4. Pilih Aktifkan.
5. Di jendela pop-up, pilih Permintaan untuk mengaktifkan.

AWS CLI

Untuk meminta untuk mengaktifkan pencari bukti di AWS CLI

Jalankan [perintah](#) `update-settings` dengan parameter. `--evidence-finder-enabled`

```
aws auditmanager update-settings --evidence-finder-enabled
```

Audit Manager API

Untuk meminta untuk mengaktifkan pencari bukti menggunakan API

Panggil [UpdateSettings](#) operasi dan gunakan `FinderEnabled` [parameter](#) bukti.

Untuk informasi selengkapnya, pilih tautan sebelumnya untuk membaca lebih lanjut di Referensi API Manajer Audit. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasa AWS .

Langkah selanjutnya

Setelah meminta untuk mengaktifkan pencari bukti, Anda dapat memeriksa status permintaan Anda. Untuk petunjuk, lihat [Mengkonfirmasi status pencari bukti](#).

Sumber daya tambahan

- [Pencari bukti](#)
- [Memecahkan masalah pencari bukti](#)

Mengkonfirmasi status pencari bukti

Setelah Anda mengirimkan permintaan untuk mengaktifkan pencari bukti, dibutuhkan waktu hingga 10 menit untuk mengaktifkan fitur dan membuat penyimpanan data peristiwa. Segera setelah penyimpanan data peristiwa dibuat, semua bukti baru dicerna ke penyimpanan data peristiwa ke depan.

Ketika pencari bukti diaktifkan dan penyimpanan data peristiwa dibuat, kami mengisi kembali penyimpanan data peristiwa yang baru dibuat dengan bukti masa lalu Anda hingga dua

tahun. Proses ini terjadi secara otomatis dan membutuhkan waktu hingga tujuh hari untuk menyelesaikannya.

Ikuti langkah-langkah di halaman ini untuk memeriksa dan memahami status permintaan Anda untuk mengaktifkan pencari bukti.

Prasyarat

Pastikan Anda mengikuti langkah-langkah untuk mengaktifkan pencari bukti. Untuk petunjuk, lihat [Mengaktifkan pencari bukti](#).

Prosedur

Anda dapat memeriksa status pencari bukti saat ini menggunakan konsol Audit Manager AWS CLI, atau API Manajer Audit.

Audit Manager console

Untuk melihat status pencari bukti saat ini di konsol Audit Manager

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Pada panel navigasi kiri, pilih Pengaturan.
3. Di bawah Aktifkan pencari bukti — opsional, tinjau status saat ini.

Setiap status didefinisikan sebagai berikut:

Status	Deskripsi
Pencari bukti tidak diaktifkan	Anda belum berhasil mengaktifkan pencari bukti.
Anda telah meminta untuk mengaktifkan pencari bukti	Permintaan Anda sedang menunggu penyimpanan data acara yang sedang dibuat.
Pencari bukti diaktifkan	Penyimpanan data acara dibuat. Anda sekarang dapat menggunakan pencari bukti. Tergantung berapa banyak bukti yang Anda miliki, dibutuhkan waktu hingga tujuh hari untuk mengisi kembali penyimpanan

Status	Deskripsi
	an data peristiwa baru dengan data bukti masa lalu Anda. Panel informasi biru menunjukkan bahwa pengisian ulang data sedang berlangsung. Jangan ragu untuk mulai menjelajahi pencari bukti sementara itu. Namun, perlu diingat bahwa tidak semua data tersedia sampai isi ulang selesai.
Anda telah meminta untuk menonaktifkan pencari bukti	Permintaan Anda sedang menunggu penyimpanan data acara dihapus.
Pencari bukti telah dinonaktifkan	Pencari bukti telah dinonaktifkan secara permanen dan penyimpanan data peristiwa dihapus.

AWS CLI

Untuk melihat status pencari bukti saat ini di AWS CLI

Jalankan [perintah](#) `get-settings` dengan `--attribute` parameter disetel ke `EVIDENCE_FINDER_ENABLEMENT`

```
aws auditmanager get-settings --attribute EVIDENCE_FINDER_ENABLEMENT
```

Ini mengembalikan informasi berikut:

Status pengaktifan

Atribut ini menunjukkan status pencari bukti saat ini.

- **ENABLE_IN_PROGRESS**— Anda meminta untuk mengaktifkan pencari bukti. Penyimpanan data peristiwa saat ini sedang dibuat untuk mendukung kueri pencari bukti.
- **ENABLED**— Penyimpanan data peristiwa dibuat dan pencari bukti diaktifkan. Sebaiknya tunggu tujuh hari sampai penyimpanan data acara diisi ulang dengan data bukti masa lalu Anda. Anda dapat menggunakan pencari bukti sementara itu, tetapi tidak semua data tersedia sampai pengisian ulang selesai.
- **DISABLE_IN_PROGRESS**— Anda meminta untuk menonaktifkan pencari bukti, dan permintaan Anda menunggu penyimpanan data acara dihapus.

- **DISABLED**— Anda menonaktifkan pencari bukti secara permanen dan penyimpanan data peristiwa dihapus. Anda tidak dapat mengaktifkan kembali pencari bukti setelah titik ini.

Status Pengisian Kembali

Atribut ini menunjukkan status pengisian ulang data bukti saat ini.

- **NOT_STARTED**— Pengisian ulang belum dimulai.
- **IN_PROGRESS**— Pengisian ulang sedang berlangsung. Ini membutuhkan waktu hingga tujuh hari untuk menyelesaikannya, tergantung pada jumlah data bukti.
- **COMPLETED**— Isi ulang selesai. Semua bukti masa lalu Anda sekarang dapat ditanyakan.

Audit Manager API

Untuk melihat status pencari bukti saat ini menggunakan API

Panggil [GetSettings](#) operasi dengan `attribute` parameter disetel ke `EVIDENCE_FINDER_ENABLEMENT`. Ini mengembalikan informasi berikut:

Status pengaktifan

Atribut ini menunjukkan status pencari bukti saat ini.

- **ENABLE_IN_PROGRESS**- Anda meminta untuk mengaktifkan pencari bukti. Penyimpanan data peristiwa saat ini sedang dibuat untuk mendukung kueri pencari bukti.
- **ENABLED**- Penyimpanan data peristiwa telah dibuat dan pencari bukti diaktifkan. Sebaiknya tunggu tujuh hari sampai penyimpanan data acara diisi ulang dengan data bukti masa lalu Anda. Anda dapat menggunakan pencari bukti sementara itu, tetapi tidak semua data tersedia sampai pengisian ulang selesai.
- **DISABLE_IN_PROGRESS**- Anda meminta untuk menonaktifkan pencari bukti, dan permintaan Anda sedang menunggu penghapusan penyimpanan data acara.
- **DISABLED**- Anda menonaktifkan pencari bukti secara permanen dan penyimpanan data peristiwa dihapus. Anda tidak dapat mengaktifkan kembali pencari bukti setelah titik ini.

Status Pengisian Kembali

Atribut ini menunjukkan status pengisian ulang data bukti saat ini.

- NOT_STARTED berarti pengisian ulang belum dimulai.
- IN_PROGRESS berarti bahwa pengisian ulang sedang berlangsung. Ini membutuhkan waktu hingga tujuh hari untuk menyelesaikannya, tergantung pada jumlah data bukti.
- COMPLETED berarti bahwa isi ulang selesai. Semua bukti masa lalu Anda sekarang dapat ditanyakan.

Untuk informasi selengkapnya, lihat [bukti FinderEnablement](#) di Referensi API Manajer Audit.

Langkah selanjutnya

Setelah pencari bukti berhasil diaktifkan, Anda dapat mulai menggunakan fitur ini. Sebaiknya tunggu tujuh hari sampai penyimpanan data acara diisi ulang dengan data bukti masa lalu Anda. Anda dapat menggunakan pencari bukti sementara itu, tetapi tidak semua data mungkin tersedia sampai pengisian ulang selesai.

Untuk memulai dengan pencari bukti, lihat [Mencari bukti di pencari bukti](#).

Sumber daya tambahan

- [Memecahkan masalah pencari bukti](#)

Menonaktifkan pencari bukti

Jika Anda tidak ingin lagi menggunakan pencari bukti, Anda dapat menonaktifkan fitur tersebut kapan saja.

Ikuti langkah-langkah ini untuk mempelajari cara menonaktifkan pencari bukti. Perhatikan prasyarat, karena Anda memerlukan izin khusus untuk menghapus penyimpanan data peristiwa di CloudTrail Lake yang dibuat saat Anda mengaktifkan pencari bukti.

Prasyarat

Izin yang diperlukan untuk menonaktifkan pencari bukti

Untuk menonaktifkan pencari bukti, Anda memerlukan izin untuk menghapus penyimpanan data peristiwa di CloudTrail Lake. Untuk contoh kebijakan yang dapat Anda gunakan, lihat [Izin untuk menonaktifkan pencari bukti](#).

Jika Anda memerlukan bantuan dengan izin, hubungi AWS administrator Anda. Jika Anda seorang AWS administrator, Anda dapat [melampirkan pernyataan izin yang diperlukan ke kebijakan](#) IAM.

Prosedur

Anda dapat menyelesaikan tugas ini menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API.

Warning

Menonaktifkan pencari bukti akan menghapus penyimpanan data peristiwa CloudTrail Lake yang dibuat oleh Audit Manager. Akibatnya, Anda tidak dapat mengaktifkan kembali fitur tersebut. Untuk menggunakan kembali pencari bukti setelah Anda menonaktifkannya, Anda harus [menonaktifkan AWS Audit Manager](#), dan kemudian [mengaktifkan kembali layanan](#) sepenuhnya.

Audit Manager console

Untuk menonaktifkan pencari bukti di konsol Audit Manager

1. Di bagian Pen cari bukti pada halaman pengaturan Manajer Audit, pilih Non aktifkan.
2. Di jendela pop-up yang muncul, masukkan **Yes** untuk mengonfirmasi keputusan Anda.
3. Pilih Per mintaan untuk menonaktifkan.

AWS CLI

Untuk menonaktifkan pencari bukti di AWS CLI

Jalankan [perintah](#) `update-settings` dengan parameter. `--no-evidence-finder-enabled`

```
aws auditmanager update-settings --no-evidence-finder-enabled
```

Audit Manager API

Untuk menonaktifkan pencari bukti menggunakan API

Panggil [UpdateSettings](#) operasi dan gunakan FinderEnabled [parameter](#) bukti.

Untuk informasi selengkapnya, pilih tautan sebelumnya untuk membaca lebih lanjut di Referensi API Manajer Audit. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu SDK khusus bahasa AWS .

Sumber daya tambahan

- [Memecahkan masalah pencari bukti](#)

Mengkonfigurasi tujuan ekspor default Anda untuk pencari bukti

Saat menjalankan kueri di pencari bukti, Anda dapat mengekspor hasil penelusuran ke file nilai yang dipisahkan koma (CSV). Gunakan pengaturan ini untuk memilih bucket S3 default tempat Audit Manager menyimpan file yang diekspor.

Prasyarat

Bucket S3 Anda harus memiliki kebijakan izin yang diperlukan CloudTrail untuk mengizinkan menulis file ekspor ke dalamnya. Lebih khusus lagi, kebijakan bucket harus menyertakan `s3:PutObject` tindakan dan bucket ARN, dan daftar CloudTrail sebagai prinsipal layanan.

- Untuk contoh kebijakan izin yang dapat Anda gunakan, lihat [Resource-based Contoh kebijakan untuk AWS Audit Manager](#).
- Untuk petunjuk untuk melampirkan kebijakan ini ke bucket S3 Anda, lihat Men [ambahkan kebijakan bucket menggunakan konsol Amazon S3](#).
- Untuk tips selengkapnya, lihat kiat [konfigurasi untuk tujuan ekspor Anda](#) di halaman ini.

Kiat konfigurasi untuk tujuan ekspor Anda

Untuk memastikan ekspor file berhasil, kami sarankan Anda memverifikasi konfigurasi berikut untuk tujuan ekspor Anda.

Wilayah AWS

K Wilayah AWS unci yang dikelola pelanggan Anda (jika Anda menyediakannya) harus sesuai dengan Wilayah penilaian Anda. Untuk petunjuk tentang cara mengubah kunci KMS Anda, lihat pengaturan [enkripsi data](#) Audit Manager.

Cross-account Bucket S3

Menggunakan bucket S3 lintas akun sebagai tujuan ekspor Anda tidak didukung di konsol Audit Manager. Dimungkinkan untuk menentukan bucket lintas akun menggunakan AWS CLI atau salah satu AWS SDK, tetapi untuk kesederhanaan, kami menyarankan Anda untuk tidak melakukan ini. Jika Anda memilih untuk menggunakan bucket S3 lintas akun sebagai tujuan ekspor, pertimbangkan hal-hal berikut.

- Secara default, objek S3 — seperti ekspor CSV — dimiliki oleh yang mengunggah objek. Akun AWS Anda dapat menggunakan [set](#) elan Kepemilikan Objek S3 untuk mengubah perilaku default ini, sehingga setiap objek baru yang ditulis oleh akun dengan daftar `bucket-owner-full-control` kontrol akses tersimpan (ACL) secara otomatis menjadi milik pemilik bucket.

Meskipun ini bukan persyaratan, kami sarankan Anda membuat perubahan berikut pada pengaturan bucket lintas akun Anda. Membuat perubahan ini memastikan bahwa pemilik bucket memiliki kontrol penuh atas file yang diekspor yang Anda publikasikan ke bucket mereka.

- [Tetapkan kepemilikan objek bucket S3](#) ke bucket owner yang lebih disukai, bukan penulis objek default
- [Tambahkan kebijakan bucket](#) untuk memastikan bahwa objek yang diunggah ke bucket tersebut memiliki `bucket-owner-full-control` ACL
- Untuk mengizinkan Audit Manager mengeksport file ke bucket S3 lintas akun, Anda harus menambahkan kebijakan bucket S3 berikut ke bucket tujuan ekspor Anda. Ganti *placeholder text* dengan informasi Anda sendiri. PrincipalElemen dalam kebijakan ini adalah pengguna atau peran yang memiliki penilaian dan mengeksport file. Men Resource entukan bucket S3 lintas akun tempat file diekspor.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow cross account file exports",
      "Effect": "Allow",
      "Principal": {
        "AWS":
          "arn:aws:iam::111122223333:user/AssessmentOwnerUserName"
      },
      "Action": [
```

```

        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:PutObjectAcl",
        "s3:DeleteObject"
    ],
    "Resource": [
        "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
        "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
    ]
}
]
}

```

Prosedur

Anda dapat memperbarui setelan ini menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API.

Audit Manager console

Untuk memperbarui setelan tujuan ekspor Anda di konsol Audit Manager

1. Dari tab pengaturan pencari bukti, buka bagian tujuan ekspor.
2. Pilih salah satu opsi berikut:
 - Jika Anda ingin menghapus bucket S3 saat ini, pilih Hapus untuk menghapus pengaturan Anda.
 - Jika Anda ingin menyimpan bucket S3 default untuk pertama kalinya, lanjutkan ke langkah 3.
3. Tentukan bucket S3 tempat Anda ingin menyimpan file yang diekspor.
 - Pilih Browse S3 untuk memilih dari daftar bucket Anda.
 - Atau, Anda dapat memasukkan URI bucket dalam format ini: **s3://bucketname/prefix**

 Tip

Agar bucket tujuan tetap teratur, Anda dapat membuat folder opsional untuk ekspor CSV Anda. Untuk melakukannya, tambahkan garis miring (/) dan awalan ke nilai di kotak URI Sumber Daya (misalnya, `/evidenceFinderCSVExports`). Audit Manager kemudian menyertakan awalan ini ketika menambahkan file CSV ke bucket, dan Amazon S3 menghasilkan jalur yang ditentukan oleh awalan. Untuk informasi selengkapnya tentang awalan di Amazon S3, lihat [Mengatur objek di konsol Amazon S3](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

4. Setelah selesai, pilih Simpan.

Untuk petunjuk tentang cara membuat bucket S3, lihat [Membuat bucket](#) di Panduan Pengguna Amazon S3.

AWS CLI

Untuk memperbarui pengaturan tujuan ekspor Anda di AWS CLI

Jalan [kan](#) perintah `update-settings` dan gunakan `--default-export-destination` parameter untuk menentukan bucket S3.

Dalam contoh berikut, ganti *placeholder text* dengan informasi Anda sendiri:

```
aws auditmanager update-settings --default-export-destination
destinationType=S3,destination=amzn-s3-demo-destination-bucket
```

Untuk petunjuk tentang cara membuat bucket S3, lihat [create-bucket](#) di Referensi Perintah AWS CLI .

Audit Manager API

Untuk memperbarui setelan tujuan ekspor menggunakan API

Panggil [UpdateSettings](#) operasi dan gunakan `ExportDestination` [parameter](#) default untuk menentukan bucket S3.

Untuk petunjuk tentang cara membuat bucket S3, lihat [CreateBucket](#) di Referensi API Amazon S3.

Pemberitahuan di AWS Audit Manager

AWS Audit Manager dapat memberi tahu Anda tentang tindakan pengguna melalui [Amazon Simple Notification Service \(Amazon SNS\)](#).

Audit Manager mengirimkan pemberitahuan ketika salah satu peristiwa berikut terjadi:

- Pemilik audit mendelegasikan set kontrol untuk ditinjau.
- Delegasi mengirimkan kontrol yang ditinjau kembali ke pemilik audit.
- Pemilik audit menyelesaikan peninjauan set kontrol.

Sumber daya tambahan

- Untuk mengonfigurasi notifikasi di Audit Manager, lihat [Mengkonfigurasi notifikasi Audit Manager](#).
- Untuk menemukan jawaban atas pertanyaan dan masalah umum, lihat [Memecahkan masalah pemberitahuan](#) di bagian Pemecahan Masalah di panduan ini.

Memecahkan masalah umum di AWS Audit Manager

Saat Anda menggunakan AWS Audit Manager, Anda mungkin menghadapi masalah atau tantangan tertentu yang memerlukan pemecahan masalah. Baik Anda menghadapi tantangan dalam menyiapkan penilaian, mengumpulkan bukti, atau aspek layanan lainnya, Anda dapat menggunakan panduan pemecahan masalah ini untuk menemukan rekomendasi kami yang membantu Anda menyelesaikan masalah umum dengan cepat dan efisien.

Kami mendorong Anda untuk meninjau daftar topik di bawah ini, menemukan topik yang paling sesuai dengan skenario Anda, dan ikuti panduan yang diberikan untuk kembali ke jalurnya. Dengan mengikuti langkah-langkah pemecahan masalah yang disediakan, Anda mungkin dapat menyelesaikan masalah secara mandiri dan terus memanfaatkan kemampuan penuh Manajer Audit. Namun, jika masalah spesifik Anda tidak tercakup di sini, atau Anda tidak dapat menyelesaikannya setelah mengikuti langkah-langkah yang disarankan, kami sarankan Anda menghubungi [Dukungan](#) untuk mendapatkan bantuan lebih lanjut.

Topik

- [Memecahkan masalah penilaian dan pengumpulan bukti](#)
- [Memecahkan masalah laporan penilaian](#)
- [Memecahkan masalah kontrol dan pengaturan kontrol](#)
- [Memecahkan masalah dasbor](#)
- [Pemecahan masalah administrator yang didelegasikan dan AWS Organizations masalah](#)
- [Memecahkan masalah pencari bukti](#)
- [Memecahkan masalah kerangka kerja](#)
- [Memecahkan masalah pemberitahuan](#)
- [Memecahkan masalah izin dan akses](#)

Memecahkan masalah penilaian dan pengumpulan bukti

Anda dapat menggunakan informasi di halaman ini untuk menyelesaikan masalah penilaian umum dan pengumpulan bukti di Manajer Audit.

Masalah pengumpulan bukti

- [Saya membuat penilaian tetapi saya belum dapat melihat bukti](#)
- [Penilaian saya tidak mengumpulkan bukti pemeriksaan kepatuhan dari AWS Security Hub CSPM](#)
- [Penilaian saya tidak mengumpulkan bukti pemeriksaan kepatuhan dari AWS Config](#)
- [Penilaian saya tidak mengumpulkan bukti aktivitas pengguna dari AWS CloudTrail](#)
- [Penilaian saya tidak mengumpulkan bukti data konfigurasi untuk AWS Panggilan API](#)
- [Kontrol umum tidak mengumpulkan bukti otomatis](#)
- [Bukti saya dihasilkan pada interval yang berbeda, dan saya tidak yakin seberapa sering itu dikumpulkan](#)
- [Saya menonaktifkan dan kemudian mengaktifkan kembali Manajer Audit, dan sekarang penilaian saya yang sudah ada sebelumnya tidak lagi mengumpulkan bukti](#)
- [Di halaman detail penilaian saya, saya diminta untuk membuat ulang penilaian saya](#)
- [Apa perbedaan antara sumber data dan sumber bukti?](#)

Masalah penilaian

- [Pembuatan penilaian saya gagal](#)
- [Apa yang terjadi jika saya menghapus akun dalam lingkup dari organisasi saya?](#)
- [Saya tidak dapat melihat layanan dalam lingkup penilaian saya](#)
- [Saya tidak dapat mengedit layanan dalam lingkup penilaian saya](#)
- [Apa perbedaan antara layanan dalam ruang lingkup dan tipe sumber data?](#)

Saya membuat penilaian tetapi saya belum dapat melihat bukti

Jika Anda tidak dapat melihat bukti apa pun, kemungkinan Anda tidak menunggu setidaknya 24 jam setelah Anda membuat penilaian atau ada kesalahan konfigurasi.

Kami menyarankan Anda memeriksa yang berikut ini:

1. Pastikan bahwa 24 jam berlalu sejak Anda membuat penilaian. Bukti otomatis tersedia 24 jam setelah Anda membuat penilaian.
2. Pastikan Anda menggunakan Audit Manager Wilayah AWS sama dengan Layanan AWS yang Anda harapkan untuk melihat buktinya.

3. Jika Anda mengharapkan untuk melihat bukti pemeriksaan kepatuhan dari AWS Config dan AWS Security Hub CSPM, pastikan konsol CSPM Security Hub AWS Config dan konsol CSPM menampilkan hasil untuk pemeriksaan ini. Hasil CSPM AWS Config dan Security Hub harus ditampilkan dengan cara yang sama dengan Wilayah AWS yang Anda gunakan Audit Manager.

Jika Anda masih tidak dapat melihat bukti dalam penilaian Anda dan itu bukan karena salah satu masalah ini, periksa penyebab potensial lainnya yang dijelaskan di halaman ini.

Penilaian saya tidak mengumpulkan bukti pemeriksaan kepatuhan dari AWS Security Hub CSPM

Jika Anda tidak melihat bukti pemeriksaan kepatuhan untuk AWS Security Hub CSPM kontrol, ini bisa disebabkan oleh salah satu masalah berikut.

Konfigurasi yang hilang di AWS Security Hub CSPM

Masalah ini dapat disebabkan jika Anda melewati beberapa langkah konfigurasi saat Anda mengaktifkan AWS Security Hub CSPM.

Untuk memperbaiki masalah ini, pastikan Anda mengaktifkan Security Hub CSPM dengan pengaturan yang diperlukan untuk Audit Manager. Untuk petunjuk, lihat [Aktifkan dan mengatur AWS Security Hub CSPM](#).

Nama kontrol CSPM Hub Keamanan tidak dimasukkan dengan benar di **ControlMappingSource**

Saat Anda menggunakan Audit Manager API untuk membuat kontrol kustom, Anda dapat menentukan kontrol CSPM Security Hub sebagai pemetaan sumber [data](#) untuk pengumpulan bukti. Untuk melakukan ini, Anda memasukkan ID kontrol sebagai [keywordValue](#).

Jika Anda tidak melihat bukti pemeriksaan kepatuhan untuk kontrol CSPM Security Hub, bisa jadi itu salah dimasukkan dalam kontrol Anda. `keywordValue ControlMappingSource` `keywordValue` ini peka huruf besar/kecil. Jika Anda salah memasukkannya, Audit Manager mungkin tidak mengenali aturan itu. Akibatnya, Anda mungkin tidak mengumpulkan bukti pemeriksaan kepatuhan untuk kontrol tersebut seperti yang diharapkan.

Untuk memperbaiki masalah ini, [perbarui kontrol khusus](#) dan `revisikeywordValue`. Format kata kunci CSPM Security Hub yang benar bervariasi. Untuk akurasi, referensi daftar [Kontrol CSPM Security Hub yang didukung](#).

AuditManagerSecurityHubFindingsReceiverA EventBridge turan Amazon hilang

Saat Anda mengaktifkan Audit Manager, aturan bernama otomatis AuditManagerSecurityHubFindingsReceiver dibuat dan diaktifkan di Amazon EventBridge. Aturan ini memungkinkan Audit Manager mengumpulkan temuan Security Hub CSPM sebagai bukti.

Jika aturan ini tidak terdaftar dan diaktifkan di Wilayah AWS tempat Anda menggunakan CSPM Hub Keamanan, Audit Manager tidak dapat mengumpulkan temuan CSPM Hub Keamanan untuk Wilayah tersebut.

Untuk mengatasi masalah ini, buka [EventBridge konsol](#) dan konfirmasikan bahwa AuditManagerSecurityHubFindingsReceiver aturan ada di konsol Anda Akun AWS. Jika aturan tidak ada, sebaiknya non [aktifkan Audit Manager](#) lalu mengaktifkan kembali layanan. Jika tindakan ini tidak menyelesaikan masalah, atau jika menonaktifkan Audit Manager bukan pilihan, [hubungi Dukungan](#) untuk mendapatkan bantuan.

Service-linked AWS Config aturan yang dibuat oleh Security Hub CSPM

Perlu diingat bahwa Audit Manager tidak mengumpulkan bukti dari AWS Config aturan [terkait layanan yang dibuat oleh Security Hub C](#) SPM. Ini adalah jenis AWS Config aturan terkelola tertentu yang diaktifkan dan dikendalikan oleh layanan CSPM Security Hub. Security Hub CSPM membuat instance aturan terkait layanan ini di AWS lingkungan Anda, bahkan jika instance lain dari aturan yang sama sudah ada. Akibatnya, untuk mencegah duplikasi bukti, Audit Manager tidak mendukung pengumpulan bukti dari aturan terkait layanan.

Saya menonaktifkan kontrol keamanan di Security Hub CSPM. Apakah Audit Manager mengumpulkan bukti pemeriksaan kepatuhan untuk kontrol keamanan itu?

Audit Manager tidak mengumpulkan bukti untuk kontrol keamanan yang dinonaktifkan.

Jika Anda menyetel status kontrol keamanan menjadi [dininonaktifkan](#) di Security Hub CSPM, tidak ada pemeriksaan keamanan yang dilakukan untuk kontrol tersebut di akun saat ini dan Wilayah. Akibatnya, tidak ada temuan keamanan yang tersedia di Security Hub CSPM, dan tidak ada bukti terkait yang dikumpulkan oleh Manajer Audit.

Dengan menghormati status dinonaktifkan yang Anda tetapkan di Security Hub CSPM, Audit Manager memastikan bahwa penilaian Anda secara akurat mencerminkan kontrol keamanan aktif

dan temuan yang relevan dengan lingkungan Anda, tidak termasuk kontrol yang sengaja Anda nonaktifkan.

Saya mengatur status temuan ke Suppressed di Security Hub CSPM. Apakah Manajer Audit mengumpulkan bukti pemeriksaan kepatuhan tentang temuan itu?

Manajer Audit mengumpulkan bukti untuk kontrol keamanan yang telah menekan temuan.

Jika Anda menyetel status alur kerja temuan ke [ditekan](#) di Security Hub CSPM, ini berarti Anda meninjau temuan tersebut dan tidak percaya bahwa tindakan apa pun diperlukan. Di Manajer Audit, temuan yang ditekan ini dikumpulkan sebagai bukti dan dilampirkan pada penilaian Anda. Rincian bukti menunjukkan status evaluasi yang SUPPRESSED dilaporkan langsung dari Security Hub CSPM.

Pendekatan ini memastikan bahwa penilaian Manajer Audit Anda secara akurat mewakili temuan dari Security Hub CSPM, sementara juga memberikan visibilitas ke dalam setiap temuan yang ditekan yang mungkin memerlukan tinjauan atau pertimbangan lebih lanjut dalam audit.

Penilaian saya tidak mengumpulkan bukti pemeriksaan kepatuhan dari AWS Config

Jika Anda tidak melihat bukti pemeriksaan kepatuhan untuk suatu AWS Config aturan, ini bisa disebabkan oleh salah satu masalah berikut.

Pengidentifikasi aturan tidak dimasukkan dengan benar di **ControlMappingSource**

Saat Anda menggunakan Audit Manager API untuk membuat kontrol kustom, Anda dapat menentukan AWS Config aturan sebagai pemetaan sumber [data](#) untuk pengumpulan bukti. [keywordValue](#) Yang Anda tentukan tergantung pada jenis aturan.

Jika Anda tidak melihat bukti pemeriksaan kepatuhan untuk suatu AWS Config aturan, bisa jadi keywordValue itu salah dimasukkan dalam aturan AndaControlMappingSource. keywordValue ini peka huruf besar/kecil. Jika Anda salah memasukkannya, Audit Manager mungkin tidak mengenali aturan. Akibatnya, Anda mungkin tidak mengumpulkan bukti pemeriksaan kepatuhan untuk aturan tersebut sebagaimana dimaksud.

Untuk memperbaiki masalah ini, [perbarui kontrol khusus](#) dan revisikeywordValue.

- Untuk aturan khusus, pastikan bahwa keywordValue memiliki Custom_ awalan diikuti oleh nama aturan khusus. Format nama aturan khusus dapat bervariasi. Untuk akurasi, kunjungi [AWS Config konsol](#) untuk memverifikasi nama aturan khusus Anda.
- Untuk aturan terkelola, pastikan bahwa itu keywordValue adalah pengidentifikasi aturan diALL_CAPS_WITH_UNDERSCORES. Misalnya, CLOUDWATCH_LOG_GROUP_ENCRYPTED. Untuk akurasi, lihat daftar kata kunci aturan [terkelola yang didukung](#).

 Note

Untuk beberapa aturan terkelola, pengenal aturan berbeda dari nama aturan. Misalnya, pengenal aturan untuk [restricted-ssh](#) adalah INCOMING_SSH_DISABLED. Pastikan untuk menggunakan pengenal aturan, bukan nama aturan. Untuk menemukan pengidentifikasi aturan, pilih aturan dari [daftar aturan terkelola](#) dan cari nilai Identifiernya.

Aturannya adalah aturan terkait layanan AWS Config

Anda dapat menggunakan aturan [terkelola](#) dan aturan [khusus](#) sebagai pemetaan sumber data untuk pengumpulan bukti. Namun, Manajer Audit tidak mengumpulkan bukti dari sebagian besar [aturan terkait layanan](#).

Hanya ada dua jenis aturan terkait layanan yang dikumpulkan oleh Manajer Audit:

- Service-linked aturan dari Paket Kesesuaian
- Service-linked aturan dari AWS Organizations

Audit Manager tidak mengumpulkan bukti dari aturan terkait layanan lainnya, khususnya aturan apa pun dengan Nama Sumber Daya Amazon (ARN) yang berisi awalan berikut:
`arn:aws:config:*:*:config-rule/aws-service-rule/...`

Alasan mengapa Audit Manager tidak mengumpulkan bukti dari sebagian besar AWS Config aturan terkait layanan adalah untuk mencegah bukti duplikat dalam penilaian Anda. Aturan terkait layanan adalah jenis aturan terkelola tertentu yang memungkinkan orang lain Layanan AWS membuat AWS Config aturan di akun Anda. Misalnya, [beberapa kontrol CSPM Security Hub menggunakan aturan AWS Config terkait layanan untuk menjalankan pemeriksaan keamanan](#). Untuk setiap kontrol CSPM Hub Keamanan yang menggunakan AWS Config aturan terkait layanan, Security Hub CSPM membuat instance aturan yang diperlukan di lingkungan Anda. AWS Config AWS Ini terjadi bahkan jika aturan asli sudah ada di akun Anda. Oleh karena itu, untuk

menghindari mengumpulkan bukti yang sama dari aturan yang sama dua kali, Manajer Audit mengabaikan aturan terkait layanan dan tidak mengumpulkan bukti darinya.

AWS Config tidak diaktifkan

AWS Config harus diaktifkan di Akun AWS. Setelah Anda mengatur dengan AWS Config cara ini, Manajer Audit mengumpulkan bukti setiap kali evaluasi AWS Config aturan terjadi.

Pastikan Anda mengaktifkan AWS Config di Akun AWS. Untuk petunjuk, lihat [Mengaktifkan dan mengatur AWS Config](#).

A AWS Config aturan mengevaluasi konfigurasi sumber daya sebelum Anda menyiapkan penilaian

Jika AWS Config aturan Anda diatur untuk mengevaluasi perubahan konfigurasi untuk sumber daya tertentu, Anda mungkin melihat ketidakcocokan antara evaluasi dalam AWS Config dan bukti di Manajer Audit. Ini terjadi jika evaluasi aturan terjadi sebelum Anda mengatur kontrol dalam penilaian Manajer Audit Anda. Dalam hal ini, Audit Manager tidak menghasilkan bukti sampai sumber daya yang mendasarinya berubah status lagi dan memicu evaluasi ulang aturan.

Sebagai solusinya, Anda dapat menavigasi ke aturan di AWS Config konsol dan mengevaluasi ulang aturan [secara manual](#). Ini memunculkan evaluasi baru dari semua sumber daya yang berkaitan dengan aturan itu.

Penilaian saya tidak mengumpulkan bukti aktivitas pengguna dari AWS CloudTrail

Saat Anda menggunakan Audit Manager API untuk membuat kontrol kustom, Anda dapat menentukan nama CloudTrail peristiwa sebagai pemetaan sumber [data](#) untuk pengumpulan bukti. Untuk melakukannya, Anda memasukkan nama acara sebagai [keywordValue](#).

Jika Anda tidak melihat bukti aktivitas pengguna untuk suatu CloudTrail peristiwa, bisa jadi itu salah dimasukkan dalam acara AndaControlMappingSource. keywordValue keywordValueIni peka huruf besar/kecil. Jika Anda salah memasukkannya, Audit Manager mungkin tidak mengenali nama acara. Akibatnya, Anda mungkin tidak mengumpulkan bukti aktivitas pengguna untuk acara tersebut sebagaimana dimaksud.

Untuk memperbaiki masalah ini, [perbarui kontrol khusus](#) dan revisikeywordValue. Pastikan acara ditulis sebagai serviceprefix_ActionName. Misalnya, cloudtrail_StartLogging. Untuk akurasi, tinjau Layanan AWS awalan dan nama tindakan di Referensi [Otorisasi Layanan](#).

Penilaian saya tidak mengumpulkan bukti data konfigurasi untuk AWS Panggilan API

Saat Anda menggunakan Audit Manager API untuk membuat kontrol kustom, Anda dapat menentukan panggilan AWS API sebagai pemetaan sumber [data](#) untuk pengumpulan bukti. Untuk melakukannya, Anda memasukkan panggilan API sebagai [keywordValue](#).

Jika Anda tidak melihat bukti data konfigurasi untuk panggilan AWS API, bisa jadi itu salah dimasukkan dalam panggilan AndaControlMappingSource. keywordValue Peka keywordValue huruf besar/kecil. Jika Anda salah memasukkannya, Audit Manager mungkin tidak mengenali panggilan API. Akibatnya, Anda mungkin tidak mengumpulkan bukti data konfigurasi untuk panggilan API tersebut sebagaimana dimaksud.

Untuk memperbaiki masalah ini, [perbarui kontrol khusus](#) dan revisikeywordValue. Pastikan panggilan API ditulis sebagai serviceprefix_ActionName. Misalnya, iam_ListGroups. Untuk akurasi, referensi daftar [AWS Panggilan API didukung oleh AWS Audit Manager](#).

Kontrol umum tidak mengumpulkan bukti otomatis

Saat Anda meninjau kontrol umum, Anda mungkin melihat pesan berikut: Kontrol umum ini tidak mengumpulkan bukti otomatis dari kontrol inti.

Ini berarti bahwa tidak ada sumber AWS bukti terkelola yang saat ini dapat mendukung kontrol umum ini. Akibatnya, tab Sumber bukti kosong dan tidak ada kontrol inti yang ditampilkan.

Ketika kontrol umum tidak mengumpulkan bukti otomatis, itu disebut sebagai kontrol umum manual. Kontrol umum manual biasanya memerlukan penyediaan catatan fisik dan tanda tangan, atau detail tentang peristiwa yang terjadi di luar AWS lingkungan Anda. Untuk alasan ini, seringkali tidak ada sumber AWS data yang dapat menghasilkan bukti untuk mendukung persyaratan kontrol.

Jika kontrol umum adalah manual, Anda masih dapat menggunakannya sebagai sumber bukti untuk kontrol kustom. Satu-satunya perbedaan adalah bahwa kontrol umum tidak akan mengumpulkan bukti apa pun secara otomatis. Sebagai gantinya, Anda harus mengunggah bukti Anda sendiri secara manual untuk mendukung persyaratan kontrol umum.

Untuk menambahkan bukti ke kontrol umum manual

1. Buat kontrol kustom

- Ikuti langkah-langkah untuk [membuat](#) atau [mengedit kontrol](#) kustom.

- Saat Anda menentukan sumber bukti pada langkah 2, pilih kontrol umum manual sebagai sumber bukti.
2. Buat kerangka kerja khusus
 - Ikuti langkah-langkah untuk [membuat](#) atau [mengedit](#) kerangka kerja khusus.
 - Saat Anda menentukan kumpulan kontrol di langkah 2, sertakan kontrol kustom baru Anda.
 3. Buat penilaian
 - Ikuti langkah-langkah untuk [membuat penilaian](#) dari kerangka kustom Anda.
 - Pada titik ini, kontrol umum manual sekarang menjadi sumber bukti dalam kontrol penilaian aktif.
 4. Unggah bukti manual
 - Ikuti langkah-langkah untuk [menambahkan bukti manual](#) ke kontrol dalam penilaian Anda.

 Note

Karena lebih banyak sumber AWS data tersedia di masa depan, ada kemungkinan bahwa itu AWS mungkin memperbarui kontrol umum untuk memasukkan kontrol inti sebagai sumber bukti. Dalam hal ini, jika kontrol umum adalah sumber bukti dalam satu atau lebih kontrol penilaian aktif Anda, Anda akan mendapat manfaat dari pembaruan ini secara otomatis. Tidak diperlukan pengaturan lebih lanjut dari pihak Anda, dan Anda akan mulai mengumpulkan bukti otomatis yang mendukung kontrol umum.

Bukti saya dihasilkan pada interval yang berbeda, dan saya tidak yakin seberapa sering itu dikumpulkan

Kontrol dalam penilaian Manajer Audit dipetakan ke berbagai sumber data. Setiap sumber data memiliki frekuensi pengumpulan bukti yang berbeda. Akibatnya, tidak ada jawaban yang cocok untuk semua tentang seberapa sering bukti dikumpulkan. Beberapa sumber data mengevaluasi kepatuhan, sedangkan yang lain hanya menangkap status sumber daya dan mengubah data tanpa penentuan kepatuhan.

Berikut ini adalah ringkasan dari berbagai jenis sumber data dan seberapa sering mereka mengumpulkan bukti.

Jenis sumber data	Deskripsi	Frekuensi pengumpulan bukti	Ketika kontrol ini aktif dalam penilaian
AWS CloudTrail	Melacak aktivitas pengguna tertentu.	Berkelanjutan	Audit Manager memfilter CloudTrail log Anda berdasarkan kata kunci yang Anda pilih. Log yang diproses diimpor sebagai bukti aktivitas Pengguna.
AWS Security Hub CSPM	Menangkap snapshot dari postur keamanan sumber daya Anda dengan melaporkan temuan dari Security Hub CSPM.	Berdasarkan jadwal pemeriksaan CSPM Security Hub (biasanya sekitar setiap 12 jam)	Audit Manager mengambil temuan keamanan langsung dari Security Hub CSPM. Temuan ini diimpor sebagai bukti pemeriksaan kepatuhan.
AWS Config	Menangkap snapshot dari postur keamanan sumber daya Anda dengan melaporkan temuan dari AWS Config.	Berdasarkan pengaturan yang didefinisikan dalam AWS Config aturan	Audit Manager mengambil evaluasi aturan langsung dari AWS Config. Evaluasi diimpor sebagai bukti pemeriksaan kepatuhan.
AWS Panggilan API	Mengambil snapshot konfigurasi sumber daya Anda secara langsung melalui panggilan API ke yang ditentukan Layanan AWS.	Harian, mingguan, atau bulanan	Audit Manager membuat panggilan API berdasarkan frekuensi yang Anda tentukan. Respons diimpor sebagai bukti data Konfigurasi.

Terlepas dari frekuensi pengumpulan bukti, bukti baru dikumpulkan secara otomatis selama penilaian aktif. Untuk informasi selengkapnya, lihat [Frekuensi pengumpulan bukti](#).

Untuk mempelajari selengkapnya, lihat [Jenis sumber data yang didukung untuk bukti otomatis](#) dan [Mengubah seberapa sering kontrol mengumpulkan bukti](#).

Saya menonaktifkan dan kemudian mengaktifkan kembali Manajer Audit, dan sekarang penilaian saya yang sudah ada sebelumnya tidak lagi mengumpulkan bukti

Ketika Anda menonaktifkan Audit Manager dan memilih untuk tidak menghapus data Anda, penilaian Anda yang ada akan beralih ke keadaan tidak aktif dan berhenti mengumpulkan bukti. Ini berarti bahwa ketika Anda mengaktifkan kembali Manajer Audit, penilaian yang Anda buat sebelumnya tetap tersedia. Namun, mereka tidak secara otomatis melanjutkan pengumpulan bukti.

Untuk mulai mengumpulkan bukti lagi untuk penilaian yang sudah ada sebelumnya, [edit penilaian](#) dan pilih **Simpan** tanpa membuat perubahan apa pun.

Di halaman detail penilaian saya, saya diminta untuk membuat ulang penilaian saya

Create new assessment to collect more comprehensive evidence
This assessment was created from a standard framework that now supports more evidence sources. We recommend that you create a new version of this assessment from the updated framework. Then, change the old assessment status to inactive.

[Create assessment](#)

AWS Audit Manager > Assessments > PCI DSS V3.2.1 Assessment

PCI DSS V3.2.1 Assessment [Info](#) [Edit](#) [Delete](#) [Update assessment status](#)

Assessment details

Description -			
Compliance type PCI DSS	Total evidence 6721885	Date created August 19, 2023, 00:51 (UTC+0:00)	Status Active
Assessment reports destination s3://assessment-reports-destination	Assessment report selection	Last updated October 17, 2023, 00:47 (UTC+0:00)	

Jika Anda melihat pesan yang mengatakan **Buat penilaian baru untuk mengumpulkan bukti yang lebih komprehensif**, ini menunjukkan bahwa Manajer Audit sekarang memberikan definisi baru dari kerangka standar tempat penilaian Anda dibuat.

Dalam definisi kerangka kerja baru, semua kontrol standar kerangka kerja sekarang dapat mengumpulkan bukti dari sumber yang [AWS dikelola](#). Ini berarti bahwa setiap kali ada pembaruan

ke sumber data yang mendasari untuk kontrol umum atau inti, Audit Manager secara otomatis menerapkan pembaruan yang sama ke semua kontrol standar terkait.

Untuk mendapatkan manfaat dari sumber AWS terkelola ini, kami sarankan Anda [membuat penilaian baru](#) dari kerangka kerja yang diperbarui. Setelah Anda melakukan ini, Anda kemudian dapat [mengubah status penilaian lama menjadi tidak aktif](#). Tindakan ini membantu memastikan bahwa penilaian baru Anda mengumpulkan bukti paling akurat dan komprehensif yang tersedia dari sumber ter AWS kelola. Jika Anda tidak mengambil tindakan, penilaian Anda terus menggunakan kerangka kerja lama dan definisi kontrol untuk mengumpulkan bukti persis seperti sebelumnya.

Apa perbedaan antara sumber data dan sumber bukti?

Sumber bukti menentukan dari mana bukti dikumpulkan. Ini bisa berupa sumber data individu, atau pengelompokan sumber data yang telah ditentukan yang dipetakan ke kontrol inti atau kontrol umum.

Sumber data adalah jenis sumber bukti yang paling terperinci. Sumber data mencakup rincian berikut yang memberi tahu Manajer Audit dari mana tepatnya mengumpulkan data bukti:

- [Jenis sumber data](#) (misalnya, AWS Config)
- [Pemetaan sumber data](#) (misalnya, AWS Config aturan tertentu seperti `s3-bucket-public-write-prohibited`)

Pembuatan penilaian saya gagal

Jika pembuatan penilaian Anda gagal, ini bisa disebabkan oleh salah satu masalah berikut.

Anda memilih terlalu banyak Akun AWS dalam lingkup penilaian Anda

Jika Anda menggunakan AWS Organizations, Audit Manager dapat mendukung hingga 200 akun anggota dalam lingkup satu penilaian. Jika Anda melebihi angka ini, pembuatan penilaian akan gagal.

Sebagai solusinya, Anda dapat menjalankan beberapa penilaian dengan cakupan akun yang berbeda untuk setiap penilaian hingga 250 akun anggota unik di semua penilaian.

Akun dalam lingkup Anda sudah dinilai oleh penilaian aktif lain

Jika Anda mencoba membuat penilaian yang menyertakan akun yang sudah dalam cakupan penilaian aktif lainnya, pembuatan penilaian gagal. Hal ini dapat terjadi ketika beberapa tim atau organisasi mencoba menilai akun yang sama secara bersamaan.

Anda mungkin melihat pesan kesalahan yang mirip dengan: `Scope: AWS Account [account-id] has assessments in progress.`

Untuk mengatasi masalah ini, Anda dapat mengambil salah satu tindakan berikut:

- Berkoordinasi dengan tim lain - Hubungi tim lain di organisasi Anda untuk menentukan penilaian mana yang saat ini menggunakan akun yang dimaksud. Anda kemudian dapat berkoordinasi untuk menghindari cakupan penilaian yang tumpang tindih.
- Ubah cakupan penilaian Anda - Hapus akun yang saling bertentangan dari lingkup penilaian Anda dan buat penilaian dengan akun yang tersisa. Anda dapat menilai akun yang saling bertentangan secara terpisah setelah penilaian lainnya selesai.
- Tunggu penilaian lain selesai - Jika penilaian lain bersifat sementara atau hampir selesai, Anda dapat menunggu sampai selesai sebelum membuat penilaian Anda dengan ruang lingkup yang diinginkan.

 Note

Pembatasan ini membantu memastikan bahwa pengumpulan bukti tidak bertentangan antara beberapa penilaian dan bahwa hasil audit tetap akurat dan konsisten.

Apa yang terjadi jika saya menghapus akun dalam lingkup dari organisasi saya?

Ketika akun dalam lingkup dihapus dari organisasi Anda, Manajer Audit tidak lagi mengumpulkan bukti untuk akun tersebut dan itu akan dihapus dari semua penilaian di mana akun tersebut berada dalam cakupan. Menghapus akun anggota dari semua penilaian juga akan mengurangi jumlah total akun unik dalam cakupan, memungkinkan Anda menambahkan akun baru dari organisasi Anda.

Saya tidak dapat melihat layanan dalam lingkup penilaian saya

Jika Anda tidak melihat Layanan AWS tab, ini berarti bahwa layanan dalam lingkup dikelola untuk Anda oleh Manajer Audit. Saat Anda membuat penilaian baru, Manajer Audit mengelola layanan dalam lingkup untuk Anda sejak saat itu dan seterusnya.

Jika Anda memiliki penilaian yang lebih lama, ada kemungkinan bahwa Anda melihat tab ini sebelumnya dalam penilaian Anda. Namun, Audit Manager secara otomatis menghapus tab ini dari penilaian Anda dan mengambil alih pengelolaan layanan dalam lingkup ketika salah satu peristiwa berikut terjadi:

- Anda mengedit penilaian Anda
- Anda mengedit salah satu kontrol khusus yang digunakan dalam penilaian Anda

Audit Manager menyimpulkan layanan dalam ruang lingkup dengan memeriksa kontrol penilaian Anda dan sumber datanya, dan kemudian memetakan informasi ini ke yang sesuai Layanan AWS. Jika sumber data yang mendasarinya berubah untuk penilaian Anda, kami secara otomatis memperbarui cakupan sesuai kebutuhan untuk mencerminkan layanan yang benar. Ini memastikan bahwa penilaian Anda mengumpulkan bukti yang akurat dan komprehensif tentang semua layanan yang relevan di AWS lingkungan Anda.

Saya tidak dapat mengedit layanan dalam lingkup penilaian saya

Alu [Mengedit penilaian di AWS Audit Manager](#) r kerja tidak lagi memiliki langkah Edit layanan. Ini karena Manajer Audit sekarang mengelola yang Layanan AWS berada dalam ruang lingkup penilaian Anda.

Jika Anda memiliki penilaian yang lebih lama, Anda mungkin secara manual menentukan layanan dalam cakupan saat membuat penilaian tersebut. Namun, Anda tidak dapat mengedit layanan ini ke depan. Audit Manager secara otomatis mengambil alih pengelolaan layanan dalam lingkup penilaian Anda ketika salah satu dari peristiwa berikut terjadi:

- Anda mengedit penilaian Anda
- Anda mengedit salah satu kontrol khusus yang digunakan dalam penilaian Anda

Audit Manager menyimpulkan layanan dalam ruang lingkup dengan memeriksa kontrol penilaian Anda dan sumber datanya, dan kemudian memetakan informasi ini ke yang sesuai Layanan AWS. Jika sumber data yang mendasarinya berubah untuk penilaian Anda, kami secara otomatis memperbarui cakupan sesuai kebutuhan untuk mencerminkan layanan yang benar. Ini memastikan bahwa penilaian Anda mengumpulkan bukti yang akurat dan komprehensif tentang semua layanan yang relevan di AWS lingkungan Anda.

Apa perbedaan antara layanan dalam ruang lingkup dan tipe sumber data?

A [service in scope](#) adalah Layanan AWS yang termasuk dalam lingkup penilaian Anda. Ketika layanan berada dalam cakupan, Manajer Audit mengumpulkan bukti tentang penggunaan Anda atas layanan tersebut dan sumber dayanya.

 Note

Manajer Audit mengelola yang Layanan AWS berada dalam ruang lingkup penilaian Anda. Jika Anda memiliki penilaian yang lebih lama, mungkin saja Anda secara manual menentukan layanan dalam cakupan di masa lalu. Ke depan, Anda tidak dapat menentukan atau mengedit layanan dalam cakupan.

Jenis sumber [data](#) menunjukkan dari mana tepatnya bukti dikumpulkan. Jika Anda mengunggah bukti Anda sendiri, jenis sumber datanya adalah Manual. Jika Audit Manager mengumpulkan bukti, sumber data dapat menjadi salah satu dari empat jenis.

1. AWS Security Hub CSPM — Menangkap snapshot dari postur keamanan sumber daya Anda dengan melaporkan temuan dari Security Hub CSPM.
2. AWS Config — Menangkap snapshot dari postur keamanan sumber daya Anda dengan melaporkan temuan dari AWS Config.
3. AWS CloudTrail — Melacak aktivitas pengguna tertentu untuk sumber daya.
4. AWS Panggilan API — Mengambil snapshot konfigurasi sumber daya Anda secara langsung melalui panggilan API ke tertentu Layanan AWS.

Berikut adalah dua contoh untuk menggambarkan perbedaan antara layanan dalam ruang lingkup dan tipe sumber data.

Contoh 1

Katakanlah Anda ingin mengumpulkan bukti untuk kontrol yang bernama 4.1.2 - Melarang akses penulisan publik ke bucket S3. Kontrol ini memeriksa tingkat akses kebijakan bucket S3 Anda. Untuk kontrol ini, Audit Manager menggunakan AWS Config aturan khusus ([s3-bucket-public-write-](#)) untuk mencari evaluasi bucket S3 Anda. Dalam contoh ini, berikut ini benar:

- Ini [service in scope](#) adalah Amazon S3
- Sumber [daya](#) yang sedang dinilai adalah bucket S3 Anda
- Jenis sumber [data](#) adalah AWS Config
- Pemetaan sumber [data](#) adalah AWS Config aturan tertentu (`s3-bucket-public-write-prohibited`)

Contoh 2

Katakanlah Anda ingin mengumpulkan bukti untuk kontrol HIPAA yang bernama 164.308 (a) (5) (ii) (C). Kontrol ini memerlukan prosedur pemantauan untuk mendeteksi login yang tidak tepat. Untuk kontrol ini, Audit Manager menggunakan CloudTrail log untuk mencari semua peristiwa [masuk Konsol](#) AWS Manajemen. Dalam contoh ini, berikut ini benar:

- Itu [service in scope](#) adalah IAM
- Sumber [daya](#) yang sedang dinilai adalah pengguna Anda
- Jenis sumber [data](#) adalah CloudTrail
- Pemetaan sumber [data](#) adalah CloudTrail peristiwa tertentu (ConsoleLogin)

Memecahkan masalah laporan penilaian

Anda dapat menggunakan informasi di halaman ini untuk menyelesaikan masalah laporan penilaian umum di Manajer Audit.

Topik

- [Laporan penilaian saya gagal menghasilkan](#)
- [Saya mengikuti daftar pemeriksaan di atas, dan laporan penilaian saya masih gagal menghasilkan](#)
- [Saya mendapatkan akses ditolak kesalahan saat saya mencoba membuat laporan](#)
- [Saya tidak dapat membuka zip laporan penilaian](#)
- [Ketika saya memilih nama bukti dalam laporan, saya tidak diarahkan ke detail bukti](#)
- [Pembuatan laporan penilaian saya terjebak Sedang berlangsung status, dan saya tidak yakin bagaimana ini memengaruhi penagihan saya](#)
- [Sumber daya tambahan](#)

Laporan penilaian saya gagal menghasilkan

Laporan penilaian Anda mungkin gagal dihasilkan karena sejumlah alasan. Anda dapat mulai memecahkan masalah ini dengan memeriksa penyebab yang paling sering. Gunakan daftar pemeriksaan berikut untuk memulai.

1. Periksa apakah ada Wilayah AWS informasi Anda yang tidak cocok:

- a. Apakah kunci Wilayah AWS yang dikelola pelanggan Anda cocok Wilayah AWS dengan penilaian Anda?

Jika Anda memberikan kunci KMS Anda sendiri untuk enkripsi data Audit Manager, kunci tersebut harus Wilayah AWS sama dengan penilaian Anda. Untuk mengatasi masalah ini, ubah kunci KMS menjadi kunci yang berada di Wilayah yang sama dengan penilaian Anda. Untuk petunjuk tentang cara mengubah kunci KMS, lihat [Mengkonfigurasi pengaturan enkripsi data Anda](#).

- b. Apakah kunci Wilayah AWS yang dikelola pelanggan Anda cocok Wilayah AWS dengan bucket S3 Anda?

Jika Anda memberikan kunci KMS Anda sendiri untuk enkripsi data Audit Manager, kunci tersebut harus sama Wilayah AWS dengan bucket S3 yang Anda gunakan sebagai tujuan laporan penilaian. Untuk mengatasi masalah ini, Anda dapat mengubah kunci KMS atau bucket S3 sehingga keduanya berada di Wilayah yang sama dengan penilaian Anda. Untuk petunjuk tentang cara mengubah kunci KMS, lihat [Mengkonfigurasi pengaturan enkripsi data Anda](#). Untuk petunjuk tentang cara mengubah bucket S3, lihat [Mengkonfigurasi tujuan laporan penilaian default](#).

2. Periksa izin bucket S3 yang Anda gunakan sebagai tujuan laporan penilaian:

- a. Apakah entitas IAM yang membuat laporan penilaian memiliki izin yang diperlukan untuk bucket S3?

Entitas IAM harus memiliki izin bucket S3 yang diperlukan untuk menerbitkan laporan dalam bucket tersebut. Kami memberikan [contoh kebijakan](#) yang dapat Anda gunakan.

- b. Apakah bucket S3 memiliki kebijakan bucket yang memerlukan enkripsi sisi server (SSE) menggunakan? [SSE-KMS](#)

Jika ya, kunci KMS yang digunakan dalam kebijakan bucket harus sesuai dengan kunci KMS yang ditentukan dalam setelan enkripsi data Audit Manager Anda. Jika Anda tidak mengonfigurasi kunci KMS di setelan Audit Manager, dan kebijakan bucket S3 Anda memerlukan SSE, pastikan kebijakan bucket memungkinkan [SSE-S3](#). Untuk petunjuk tentang cara mengubah kunci KMS, lihat [Mengkonfigurasi pengaturan enkripsi data Anda](#). Untuk petunjuk tentang cara mengubah bucket S3, lihat [Mengkonfigurasi tujuan laporan penilaian default](#).

Jika Anda masih tidak berhasil membuat laporan penilaian, tinjau masalah berikut di halaman ini.

Saya mengikuti daftar periksa di atas, dan laporan penilaian saya masih gagal menghasilkan

Jika laporan penilaian Anda gagal dihasilkan, penyebab yang paling mungkin adalah ukuran laporan. Sebagai solusinya, Anda dapat menghasilkan beberapa laporan penilaian daripada satu laporan penilaian yang lebih besar. Dengan melakukan ini, Anda dapat mengeksport bukti dari penilaian Anda ke dalam batch berukuran lebih mudah dikelola.

Saya mendapatkan akses ditolak kesalahan saat saya mencoba membuat laporan

Anda akan mendapatkan `access denied` kesalahan jika penilaian dibuat oleh akun administrator yang didelegasikan yang bukan milik kunci KMS yang ditentukan dalam pengaturan Manajer Audit Anda. Untuk menghindari kesalahan ini, saat Anda menunjuk administrator yang didelegasikan untuk Audit Manager, pastikan bahwa akun administrator yang didelegasikan memiliki akses pada kunci KMS yang Anda berikan saat menyiapkan Audit Manager.

Anda mungkin juga menerima `access denied` kesalahan jika Anda tidak memiliki izin menulis untuk bucket S3 yang Anda gunakan sebagai tujuan laporan penilaian.

Jika Anda mendapatkan `access denied` kesalahan, pastikan Anda memenuhi persyaratan berikut:

- Kunci KMS Anda di setelan Audit Manager memberikan izin kepada administrator yang didelegasikan. Anda dapat mengonfigurasi ini dengan mengikuti petunjuk di [Mengizinkan pengguna di akun lain menggunakan kunci KMS](#) di Panduan Peng AWS Key Management Service embang. Untuk petunjuk tentang cara meninjau dan mengubah pengaturan enkripsi Anda di Audit Manager, lihat [Mengkonfigurasi pengaturan enkripsi data Anda](#).
- Anda memiliki kebijakan izin yang memberi Anda akses menulis untuk bucket S3 yang Anda gunakan sebagai tujuan laporan penilaian. Lebih khusus lagi, kebijakan izin berisi `s3:PutObject` tindakan, menentukan ARN bucket S3, dan menyertakan kunci KMS yang digunakan untuk mengenkripsi laporan penilaian Anda. Untuk contoh kebijakan yang dapat Anda gunakan, lihat [Contoh 2 \(Izin tujuan laporan penilaian\)](#).

 Note

Jika Anda mengubah setelan enkripsi data Audit Manager, perubahan ini berlaku untuk penilaian baru yang Anda buat di masa mendatang. Ini termasuk laporan penilaian apa pun yang Anda buat dari penilaian baru Anda.

Perubahan tidak berlaku untuk penilaian yang sudah ada yang Anda buat sebelum mengubah setelan enkripsi. Ini termasuk laporan penilaian baru yang Anda buat dari penilaian yang ada, selain laporan penilaian yang ada. Penilaian yang ada — dan semua laporan penilaian mereka — terus menggunakan kunci KMS lama. Jika identitas IAM yang membuat laporan penilaian tidak memiliki izin untuk menggunakan kunci KMS lama, Anda dapat memberikan izin di tingkat kebijakan utama.

Saya tidak dapat membuka zip laporan penilaian

Jika Anda tidak dapat mengekstrak laporan penilaian di Windows, kemungkinan Windows Explorer tidak dapat mengekstraknya karena jalur file-nya memiliki beberapa folder bersarang atau nama panjang. Ini karena, di bawah sistem penamaan file Windows, jalur folder, nama file, dan ekstensi file tidak dapat melebihi 259 karakter. Jika tidak, ini menghasilkan `Destination Path Too Long` kesalahan.

Untuk mengatasi masalah ini, coba pindahkan file zip ke folder induk dari lokasi saat ini. Anda kemudian dapat mencoba lagi untuk meng-unzip dari sana. Atau, Anda juga dapat mencoba memperpendek nama file zip atau mengekstraknya ke lokasi lain yang memiliki jalur file yang lebih pendek.

Ketika saya memilih nama bukti dalam laporan, saya tidak diarahkan ke detail bukti

Masalah ini mungkin terjadi jika Anda berinteraksi dengan laporan penilaian di browser, atau menggunakan pembaca PDF default yang diinstal pada sistem operasi Anda. Beberapa browser dan pembaca PDF default sistem tidak mengizinkan pembukaan tautan relatif. Ini berarti bahwa, meskipun hyperlink mungkin berfungsi dalam PDF ringkasan laporan penilaian (seperti nama kontrol hyperlink di daftar isi), hyperlink diabaikan saat Anda mencoba menavigasi dari PDF ringkasan penilaian ke PDF detail bukti terpisah.

Jika Anda mengalami masalah ini, sebaiknya gunakan pembaca PDF khusus untuk berinteraksi dengan laporan penilaian Anda. Untuk pengalaman yang andal, kami sarankan Anda menginstal dan

menggunakan Adobe Acrobat Reader, yang dapat Anda unduh di situs web [Adobe](#). Pembaca PDF lainnya juga tersedia, tetapi Adobe Acrobat Reader telah terbukti bekerja secara konsisten dan andal dengan laporan penilaian Manajer Audit.

Pembuatan laporan penilaian saya terjebak Sedang berlangsung status, dan saya tidak yakin bagaimana ini memengaruhi penagihan saya

Pembuatan laporan penilaian tidak berdampak pada penagihan. Anda hanya ditagih berdasarkan bukti yang dikumpulkan penilaian Anda. Untuk informasi selengkapnya tentang harga, lihat [AWS Audit Manager Harga](#).

Sumber daya tambahan

Halaman-halaman berikut berisi panduan pemecahan masalah tentang menghasilkan laporan penilaian dari pencari bukti:

- [Saya tidak dapat membuat beberapa laporan penilaian dari hasil pencarian](#)
- [Saya tidak dapat memasukkan bukti spesifik dari hasil pencarian saya](#)
- [Tidak semua hasil pencari bukti saya disertakan dalam laporan penilaian](#)
- [Saya ingin membuat laporan penilaian dari hasil pencarian saya, tetapi pernyataan kueri saya gagal](#)

Memecahkan masalah kontrol dan pengaturan kontrol

Anda dapat menggunakan informasi di halaman ini untuk menyelesaikan masalah umum dengan kontrol di Audit Manager.

Masalah umum

- [Saya tidak dapat melihat kontrol atau kumpulan kontrol apa pun dalam penilaian saya](#)
- [Saya tidak dapat mengunggah bukti manual ke kontrol](#)
- [Apa artinya jika kontrol mengatakan “Penggantian tersedia”?](#)

AWS Config masalah integrasi

- [Saya perlu menggunakan beberapa AWS Config aturan sebagai sumber data untuk kontrol tunggal](#)

- [Opsis aturan khusus tidak tersedia saat saya mengonfigurasi sumber data kontrol](#)
- [Opsis aturan khusus tersedia, tetapi tidak ada aturan yang muncul di daftar dropdown](#)
- [Beberapa aturan khusus tersedia, tetapi saya tidak dapat melihat aturan yang ingin saya gunakan](#)
- [Saya tidak dapat melihat aturan terkelola yang ingin saya gunakan](#)
- [Saya ingin berbagi kerangka kerja khusus, tetapi memiliki kontrol yang menggunakan kustom AWS Config aturan sebagai sumber data. Dapatkah penerima mengumpulkan bukti untuk kontrol ini?](#)
- [Apa yang terjadi ketika aturan khusus diperbarui di AWS Config? Apakah saya perlu mengambil tindakan apa pun di Manajer Audit?](#)

Saya tidak dapat melihat kontrol atau kumpulan kontrol apa pun dalam penilaian saya

Singkatnya, untuk melihat kontrol untuk penilaian, Anda harus ditentukan sebagai pemilik audit untuk penilaian itu. Selain itu, Anda memerlukan izin IAM yang diperlukan untuk melihat dan mengelola sumber daya Audit Manager terkait.

Jika Anda memerlukan akses ke kontrol dalam penilaian, mintalah salah satu pemilik audit untuk penilaian tersebut untuk menentukan Anda sebagai pemilik audit. Anda dapat menentukan pemilik audit saat [membuat](#) atau [mengedit](#) penilaian.

Pastikan juga bahwa Anda memiliki izin yang diperlukan untuk mengelola penilaian. Kami menyarankan agar pemilik audit menggunakan [AWSAuditManagerAdministratorAccess](#) kebijakan tersebut. Jika Anda memerlukan bantuan dengan izin IAM, hubungi administrator atau [AWS Dukungan](#) Anda. Untuk informasi selengkapnya tentang cara melampirkan kebijakan ke identitas IAM, lihat Men [ambahkan Izin ke Pengguna](#) dan Men [ambahkan dan menghapus izin identitas IAM](#) di Panduan Pengguna IAM.

Saya tidak dapat mengunggah bukti manual ke kontrol

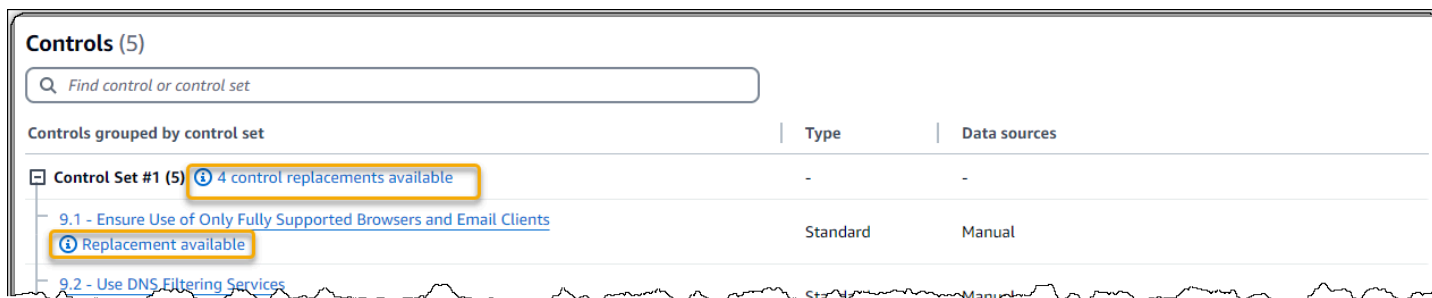
Jika Anda tidak dapat mengunggah bukti secara manual ke kontrol, kemungkinan itu karena kontrol dalam status tidak aktif.

Untuk mengunggah bukti manual ke kontrol, Anda harus terlebih dahulu mengubah status kontrol menjadi Sedang ditinjau atau Ditinjau. Untuk petunjuk, lihat [Mengubah status kontrol penilaian di AWS Audit Manager](#).

⚠ Important

Mas Akun AWS ing-masing hanya dapat mengunggah hingga 100 file bukti secara manual ke kontrol setiap hari. Melebihi kuota harian ini menyebabkan unggahan manual tambahan gagal untuk kontrol tersebut. Jika Anda perlu mengunggah sejumlah besar bukti manual ke satu kontrol, unggah bukti Anda secara berkelompok selama beberapa hari.

Apa artinya jika kontrol mengatakan “Penggantian tersedia”?



Controls grouped by control set	Type	Data sources
Control Set #1 (5) 4 control replacements available	-	-
9.1 - Ensure Use of Only Fully Supported Browsers and Email Clients Replacement available	Standard	Manual
9.2 - Use DNS Filtering Services	Standard	Manual

Jika Anda melihat pesan ini, ini berarti bahwa definisi kontrol yang diperbarui tersedia untuk satu atau lebih kontrol standar dalam kerangka kustom Anda. Kami menyarankan Anda mengganti kontrol ini sehingga Anda dapat memperoleh manfaat dari sumber bukti yang ditingkatkan yang sekarang disediakan oleh Manajer Audit.

Untuk petunjuk tentang cara melanjutkan, lihat [Pada halaman detail kerangka kerja kustom saya, saya diminta untuk membuat ulang kerangka kerja khusus saya.](#)

Saya perlu menggunakan beberapa AWS Config aturan sebagai sumber data untuk kontrol tunggal

Anda dapat menggunakan kombinasi aturan terkelola dan aturan khusus untuk satu kontrol. Untuk melakukan ini, tentukan beberapa sumber bukti untuk kontrol, dan pilih jenis aturan pilihan Anda untuk masing-masing. Anda dapat menentukan hingga 100 sumber data yang dikelola pelanggan untuk satu kontrol kustom.

Opsi aturan khusus tidak tersedia saat saya mengonfigurasi sumber data kontrol

Ini berarti Anda tidak memiliki izin untuk melihat aturan khusus untuk organisasi Anda Akun AWS atau organisasi. Lebih khusus lagi, Anda tidak memiliki izin untuk melakukan [DescribeConfigRules](#) operasi di konsol Audit Manager.

Untuk mengatasi masalah ini, hubungi AWS administrator Anda untuk mendapatkan bantuan. Jika Anda seorang AWS administrator, Anda dapat memberikan izin untuk pengguna atau grup dengan [mengelola kebijakan](#) IAM Anda.

Opsi aturan khusus tersedia, tetapi tidak ada aturan yang muncul di daftar dropdown

Ini berarti bahwa tidak ada aturan khusus yang diaktifkan dan tersedia untuk digunakan di Akun AWS organisasi Anda.

Jika Anda belum memiliki aturan khusus AWS Config, Anda dapat membuatnya. Untuk petunjuk, lihat aturan [AWS Config khusus](#) di Panduan Peng AWS Config embang.

Jika Anda mengharapkan untuk melihat aturan khusus, periksa item pemecahan masalah berikut.

Beberapa aturan khusus tersedia, tetapi saya tidak dapat melihat aturan yang ingin saya gunakan

Jika Anda tidak dapat melihat aturan khusus yang Anda harapkan untuk ditemukan, ini mungkin karena salah satu masalah berikut.

Akun Anda dikecualikan dari aturan

Ada kemungkinan bahwa akun administrator yang didelegasikan yang Anda gunakan dikecualikan dari aturan.

Akun manajemen organisasi Anda (atau salah satu akun administrator AWS Config yang didelegasikan) dapat membuat aturan organisasi khusus menggunakan AWS Command Line Interface (AWS CLI). Ketika mereka melakukannya, mereka dapat menentukan [daftar akun yang akan dikecualikan](#) dari aturan. Jika akun Anda ada di daftar ini, aturan tidak tersedia di Manajer Audit.

Untuk mengatasi masalah ini, hubungi AWS Config administrator Anda untuk mendapatkan bantuan. Jika Anda seorang AWS Config administrator, Anda dapat memperbarui daftar akun yang dikecualikan dengan menjalankan perintah [put-organization-config-rule](#).

Aturan tidak berhasil dibuat dan diaktifkan di AWS Config

Mungkin juga aturan khusus tidak berhasil dibuat dan diaktifkan. Jika terjadi [kesalahan saat membuat aturan](#), atau [aturan tidak diaktifkan](#), aturan tersebut tidak muncul dalam daftar aturan yang tersedia di Audit Manager.

Untuk bantuan terkait masalah ini, kami sarankan Anda menghubungi AWS Config administrator Anda.

Aturan adalah aturan yang dikelola

Jika Anda tidak dapat menemukan aturan yang Anda cari di bawah daftar dropdown aturan khusus, ada kemungkinan aturan tersebut adalah aturan terkelola.

Anda dapat menggunakan [AWS Config konsol](#) untuk memverifikasi apakah aturan adalah aturan terkelola. Untuk melakukannya, pilih Aturan di menu navigasi kiri dan cari aturan di tabel. Jika aturan adalah aturan terkelola, kolom Jenis menampilkan AWS dikelola.

Name	Remediation action	Type	Compliance
☐ account-part-of-organizations	Not set	AWS managed	 Compliant

Setelah mengonfirmasi bahwa itu adalah aturan terkelola, kembali ke Manajer Audit dan pilih Aturan terkelola sebagai jenis aturan. Kemudian, cari kata kunci pengenal aturan terkelola di daftar dropdown aturan terkelola.

AWS Config rule type

Info

Select a rule type to view a list of the available rules.

☒ Managed rule
Use one of the predefined rules that are provided by AWS Config.

☐ Custom rule
Use a custom rule that was created for your AWS account or organization.

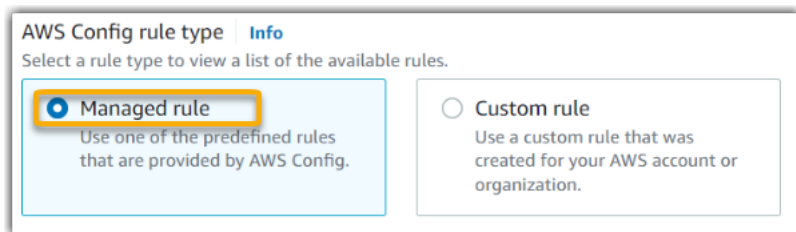
Managed rule

For information about these options, see [List of AWS Config Managed Rules](#) in the AWS Config developer guide.

ACCOUNT_PART_OF_ORGANIZATIONS

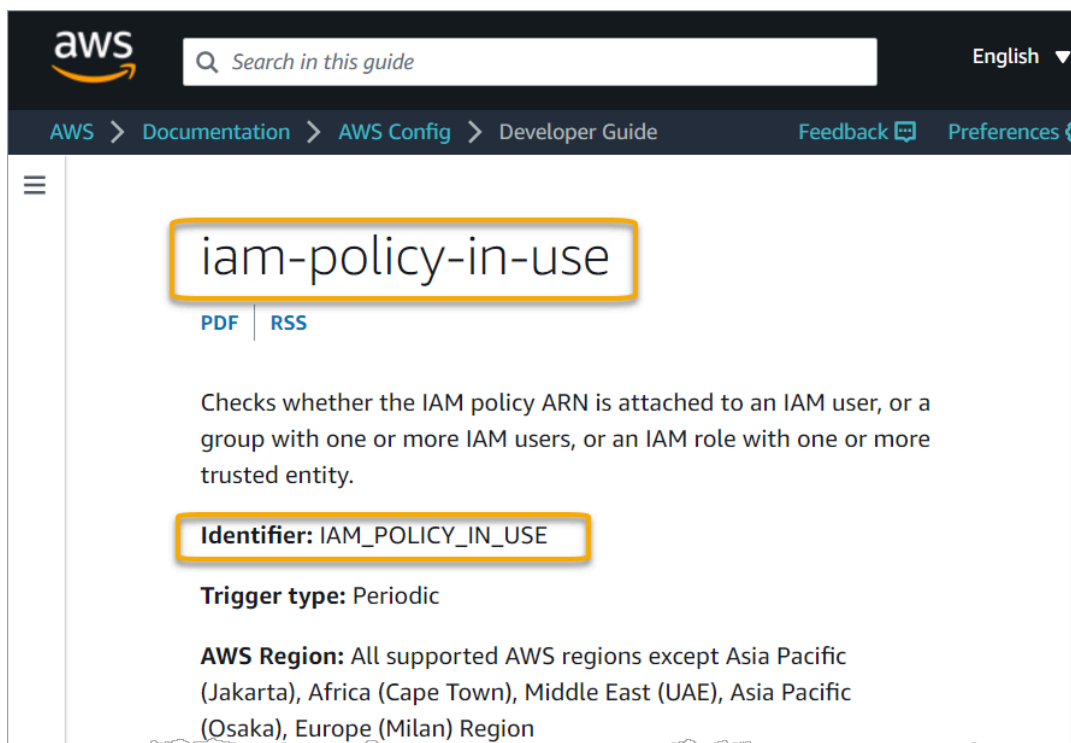
Saya tidak dapat melihat aturan terkelola yang ingin saya gunakan

Sebelum memilih aturan dari daftar dropdown di konsol Audit Manager, pastikan Anda memilih Aturan terkelola sebagai jenis aturan.

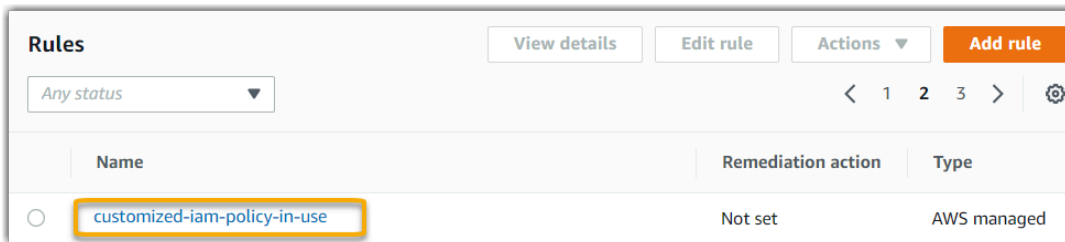


Jika Anda masih tidak dapat melihat aturan terkelola yang diharapkan untuk ditemukan, Anda mungkin mencari nama aturan tersebut. Sebagai gantinya, Anda harus mencari pengenal aturan.

Jika Anda menggunakan aturan terkelola default, nama dan pengidentifikasi serupa. Namanya dalam huruf kecil dan menggunakan tanda hubung (misalnya, `iam-policy-in-use`). Pengidentifikasi dalam huruf besar dan menggunakan garis bawah (misalnya, `IAM_POLICY_IN_USE`). Untuk menemukan pengidentifikasi aturan terkelola default, tinjau daftar kata kunci aturan terkelola yang didukung dan ikuti tautan aturan yang ingin Anda gunakan. Ini membawa Anda ke AWS Config dokumentasi untuk aturan terkelola itu. Dari sini, Anda dapat melihat nama dan pengenal. Cari kata kunci pengenal di daftar dropdown Audit Manager.

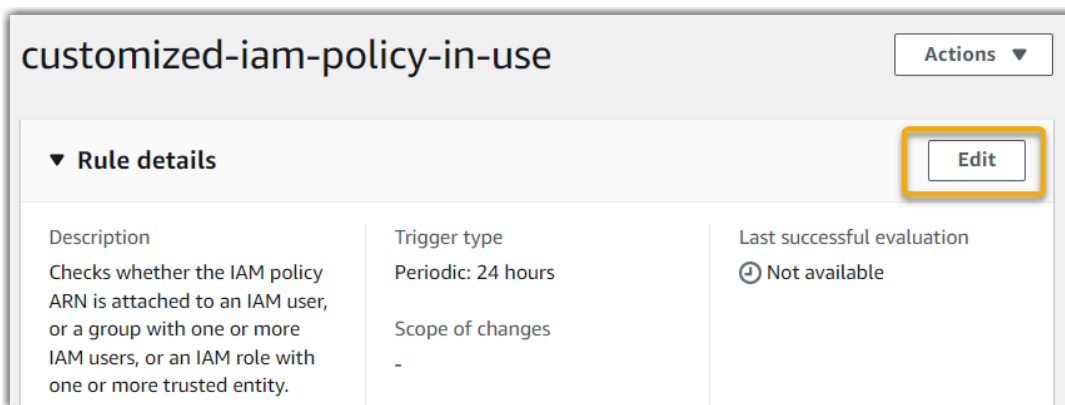


Jika Anda menggunakan aturan terkelola khusus, Anda dapat menggunakan [AWS Config konsol](#) untuk menemukan pengenalan aturan. Misalnya, katakanlah Anda ingin menggunakan aturan terkelola yang disebut `customized-iam-policy-in-use`. Untuk menemukan pengenalan untuk aturan ini, buka AWS Config konsol, pilih **Aturan** di menu navigasi kiri, dan pilih aturan di tabel.



Rules			View details	Edit rule	Actions ▼	Add rule
Any status ▼			< 1 2 3 > ⚙			
	Name	Remediation action	Type			
☐	customized-iam-policy-in-use	Not set	AWS managed			

Pilih **Edit** untuk membuka detail tentang aturan yang dikelola.



customized-iam-policy-in-use

[Actions](#) ▼

▼ Rule details

Description

Checks whether the IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity.

Trigger type

Periodic: 24 hours

Scope of changes

-

Last successful evaluation

🕒 Not available

Edit

Di bawah bagian **Detail**, Anda dapat menemukan pengidentifikasi sumber yang dibuat dari aturan terkelola (`IAM_POLICY_IN_USE`).

Edit rule

Details

Name
A unique name for the rule. 128 characters max. No special characters or spaces.

customized-iam-policy-in-use

Description

Checks whether the IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity.

Managed rule name

IAM_POLICY_IN_USE

Anda sekarang dapat kembali ke konsol Audit Manager dan memilih kata kunci pengenalan yang sama dari daftar dropdown.

AWS Config rule type [Info](#)

Select a rule type to view a list of the available rules.

☒ **Managed rule**
Use one of the predefined rules that are provided by AWS Config.

☐ **Custom rule**
Use a custom rule that was created for your AWS account or organization.

Managed rule
For information about these options, see [List of AWS Config Managed Rules](#) in the AWS Config developer guide.

IAM_POLICY_IN_USE

Saya ingin berbagi kerangka kerja khusus, tetapi memiliki kontrol yang menggunakan kustom AWS Config aturan sebagai sumber data. Dapatkah penerima mengumpulkan bukti untuk kontrol ini?

Ya, penerima dapat mengumpulkan bukti untuk kontrol ini, tetapi beberapa langkah diperlukan untuk mencapai ini.

Agar Manajer Audit mengumpulkan bukti menggunakan AWS Config aturan sebagai pemetaan sumber data, berikut ini harus benar. Ini berlaku untuk aturan terkelola dan aturan khusus.

1. Aturan harus ada di AWS lingkungan penerima

2. Aturan harus diaktifkan di AWS lingkungan penerima

Ingatlah bahwa AWS Config aturan khusus di akun Anda kemungkinan tidak ada di AWS lingkungan penerima. Selain itu, ketika penerima menerima permintaan berbagi, Audit Manager tidak membuat ulang aturan khusus apa pun di akun mereka. Agar penerima dapat mengumpulkan bukti menggunakan aturan kustom Anda sebagai pemetaan sumber data, mereka harus membuat aturan khusus yang sama di instans mereka AWS Config. Setelah penerima membuat https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_develop-rules.html dan kemudian mengaktifkan [aturan](#), Manajer Audit dapat mengumpulkan bukti dari sumber data tersebut.

Sebaiknya Anda berkomunikasi dengan penerima untuk memberi tahu mereka jika ada aturan khusus yang perlu dibuat dalam instans mereka AWS Config.

Apa yang terjadi ketika aturan khusus diperbarui di AWS Config? Apakah saya perlu mengambil tindakan apa pun di Manajer Audit?

Untuk pembaruan aturan dalam AWS lingkungan

Jika Anda memperbarui aturan khusus dalam AWS lingkungan Anda, tidak ada tindakan yang diperlukan di Manajer Audit. Audit Manager mendeteksi dan menangani pembaruan aturan seperti yang dijelaskan dalam tabel berikut. Audit Manager tidak memberi tahu Anda saat pembaruan aturan terdeteksi.

Skenario	Apa yang dilakukan oleh Audit Manager	Apa yang perlu Anda lakukan
Aturan khusus diperbarui dalam instance Anda AWS Config	Audit Manager terus melaporkan temuan untuk aturan tersebut menggunakan definisi aturan yang diperbarui.	Tidak ada tindakan yang diperlukan.
Aturan khusus dihapus di instance Anda AWS Config	Audit Manager berhenti melaporkan temuan untuk aturan yang dihapus.	Tidak ada tindakan yang diperlukan. Jika mau, Anda dapat mengedit kontrol kustom yang menggunakan aturan yang dihapus sebagai pemetaan

Skenario	Apa yang dilakukan oleh Audit Manager	Apa yang perlu Anda lakukan
		sumber data. Melakukannya membantu membersihkan pengaturan sumber data Anda dengan menghapus aturan yang dihapus. Jika tidak, nama aturan yang dihapus tetap sebagai pemetaan sumber data yang tidak digunakan.

Untuk pembaruan aturan di luar AWS lingkungan

Jika aturan khusus diperbarui di luar AWS lingkungan Anda, Audit Manager tidak mendeteksi pembaruan aturan. Ini adalah sesuatu yang perlu dipertimbangkan jika Anda menggunakan kerangka kerja khusus bersama. Ini karena, dalam skenario ini, pengirim dan penerima masing-masing bekerja di AWS lingkungan yang terpisah. Tabel berikut memberikan tindakan yang disarankan untuk skenario ini.

Peran Anda	Skenario	Tindakan yang disarankan
Sender	- Anda berbagi kerangka kerja yang menggunakan aturan khusus sebagai pemetaan sumber data. - Setelah Anda membagikan kerangka kerja, Anda memperbarui atau menghapus salah satu aturan tersebut di AWS Config.	Beri tahu penerima tentang pembaruan Anda. Dengan begitu, mereka dapat menerapkan pembaruan yang sama dan tetap sinkron dengan definisi aturan terbaru.
Penerima	- Anda menerima kerangka kerja bersama yang menggunakan aturan khusus sebagai pemetaan sumber data. - Setelah Anda membuat ulang aturan khusus di instance Anda AWS Config, pengirim	Buat pembaruan aturan yang sesuai di instance Anda sendiri AWS Config.

Peran Anda	Skenario	Tindakan yang disarankan
	memperbarui atau menghapus salah satu aturan tersebut.	

Memecahkan masalah dasbor

Anda dapat menggunakan informasi di halaman ini untuk menyelesaikan masalah dasbor umum di Audit Manager.

Topik

- [Tidak ada data di dasbor saya](#)
- [Opsional unduhan CSV tidak tersedia](#)
- [Saya tidak melihat file yang diunduh saat mencoba mengunduh file CSV](#)
- [Domain kontrol atau kontrol tertentu hilang dari dasbor](#)
- [Saya melihat kontrol serupa atau duplikat muncul di bawah domain kontrol yang sama](#)
- [Cuplikan harian menunjukkan jumlah bukti yang bervariasi setiap hari. Apakah ini normal?](#)

Tidak ada data di dasbor saya

Jika angka di [Cuplikan harian](#) widget menampilkan tanda hubung (-), ini menunjukkan bahwa tidak ada data yang tersedia. Anda harus memiliki setidaknya satu penilaian aktif untuk melihat data di dasbor. Untuk memulai, [buat penilaian](#). Setelah periode 24 jam, data penilaian Anda akan mulai muncul di dasbor.

Note

Jika angka dalam widget snapshot harian menampilkan nol (0), ini menunjukkan bahwa penilaian aktif Anda (atau penilaian yang Anda pilih) tidak memiliki bukti yang tidak sesuai.

Opsì unduhan CSV tidak tersedia

Opsì ini hanya tersedia untuk penilaian individu. Pastikan Anda menerapkan a [Filter penilaian](#) ke dasbor, lalu coba lagi. Perlu diingat bahwa Anda hanya dapat mengunduh satu file CSV pada satu waktu.

Saya tidak melihat file yang diunduh saat mencoba mengunduh file CSV

Jika domain kontrol berisi sejumlah besar kontrol, mungkin ada penundaan singkat saat Audit Manager menghasilkan file CSV. Setelah file dibuat, itu diunduh secara otomatis.

Jika Anda masih tidak melihat file yang diunduh, pastikan koneksi internet Anda berfungsi normal dan Anda menggunakan versi terbaru dari browser web Anda. Selain itu, periksa folder unduhan terbaru Anda. File diunduh ke lokasi default yang ditentukan oleh browser Anda. Jika ini tidak menyelesaikan masalah Anda, coba unduh file menggunakan browser lain.

Domain kontrol atau kontrol tertentu hilang dari dasbor

Ini mungkin berarti bahwa penilaian aktif Anda (atau penilaian tertentu) tidak memiliki data yang relevan untuk domain kontrol atau kontrol tersebut.

Domain kontrol ditampilkan di dasbor hanya jika kedua dari dua kriteria berikut terpenuhi:

- Penilaian aktif Anda (atau penilaian tertentu) berisi setidaknya satu kontrol yang terkait dengan domain tersebut
- Setidaknya satu kontrol dalam domain tersebut mengumpulkan bukti pada tanggal di bagian atas dasbor

Kontrol ditampilkan dalam domain hanya jika mengumpulkan bukti pada tanggal di bagian atas dasbor.

Saya melihat kontrol serupa atau duplikat muncul di bawah domain kontrol yang sama

Masalah ini dapat terjadi jika penilaian Anda mengumpulkan bukti dari versi berbeda dari kontrol standar yang sama.

Ini terjadi dalam skenario berikut:

Skenario 1: Anda memiliki dua penilaian yang dibuat dari kerangka standar yang sama

- Anda membuat penilaian dari kerangka standar sebelum peluncuran pustaka kontrol umum.

Penilaian ini mengumpulkan bukti menggunakan kontrol standar yang sudah ketinggalan zaman.

- Anda juga membuat penilaian dari kerangka standar yang sama setelah peluncuran pustaka kontrol umum.

Penilaian ini mengumpulkan bukti menggunakan versi baru dari kontrol standar.

- Akibatnya, penilaian Anda mengumpulkan bukti dari versi yang berbeda dari kontrol standar yang sama.

Skenario 2: Anda memiliki dua penilaian yang dibuat dari kerangka kerja khusus yang menggunakan kontrol standar

- Anda membuat penilaian dari kerangka kustom Anda sebelum peluncuran pustaka kontrol umum.

Penilaian ini mengumpulkan bukti menggunakan kontrol standar yang sudah ketinggalan zaman.

- Anda juga membuat penilaian dari kerangka kustom yang sama setelah peluncuran pustaka kontrol umum.

Penilaian ini mengumpulkan bukti menggunakan versi baru dari kontrol standar.

- Akibatnya, penilaian Anda mengumpulkan bukti dari versi yang berbeda dari kontrol standar yang sama.

Contoh: Katakanlah Anda memiliki penilaian yang sudah ada sebelumnya yang Anda buat dari kerangka standar PCI DSS sebelum 6 Juni 2024. Selain itu, Anda membuat penilaian baru dari kerangka standar PCI DSS setelah 6 Juni 2024. Akibatnya, penilaian pertama mengumpulkan bukti menggunakan versi kontrol standar yang sudah ketinggalan zaman untuk PCI DSS. Penilaian kedua mengumpulkan bukti menggunakan versi baru dari kontrol standar untuk PCI DSS. Karena kedua versi kontrol PCI DSS secara aktif mengumpulkan bukti dalam penilaian Anda, Anda mungkin akan melihat kedua set kontrol muncul di dasbor di bawah domain kontrol yang sama. Namun, dalam kasus yang jarang terjadi, kontrol usang dan kontrol baru mungkin muncul di bawah domain kontrol yang berbeda di dasbor.

Anda dapat terus mengumpulkan bukti dan melihat wawasan dasbor untuk kontrol dan kerangka kerja standar yang sudah ketinggalan zaman. Namun, kami mendorong Anda untuk menggunakan kontrol dan kerangka kerja baru yang disediakan Audit Manager setelah peluncuran pustaka kontrol umum pada 6 Juni 2024. Kontrol standar baru dapat mengumpulkan bukti dari [AWS managed source](#) s. Ini berarti bahwa setiap kali ada pembaruan ke sumber data yang mendasari untuk kontrol umum atau inti, Audit Manager secara otomatis menerapkan pembaruan yang sama ke semua kontrol standar terkait.

Cuplikan harian menunjukkan jumlah bukti yang bervariasi setiap hari.
Apakah ini normal?

Tidak semua bukti dikumpulkan setiap hari. Kontrol dalam penilaian Manajer Audit dipetakan ke sumber data yang berbeda, dan masing-masing dapat memiliki jadwal pengumpulan bukti yang berbeda. Akibatnya, diharapkan bahwa snapshot harian menampilkan sejumlah bukti yang bervariasi setiap hari. Untuk informasi selengkapnya, lihat [Frekuensi pengumpulan bukti](#).

Pemecahan masalah administrator yang didelegasikan dan AWS Organizations masalah

Anda dapat menggunakan informasi di halaman ini untuk menyelesaikan masalah administrator yang didelegasikan umum di Manajer Audit.

Topik

- [Saya tidak dapat mengatur Audit Manager dengan akun administrator yang didelegasikan](#)
- [Saat membuat penilaian, saya tidak dapat melihat akun dari organisasi saya di bawah Akun dalam cakupan](#)
- [Saya mendapatkan akses ditolak kesalahan saat saya mencoba membuat laporan penilaian menggunakan akun administrator yang didelegasikan](#)
- [Apa yang terjadi di Audit Manager jika saya memutuskan tautan akun anggota dari organisasi saya?](#)
- [Apa yang terjadi jika saya menautkan ulang akun anggota ke organisasi saya?](#)
- [Apa yang terjadi jika saya memigrasikan akun anggota dari satu organisasi ke organisasi lain?](#)

Saya tidak dapat mengatur Audit Manager dengan akun administrator yang didelegasikan

Meskipun beberapa administrator yang didelegasikan didukung AWS Organizations, Audit Manager hanya mengizinkan satu administrator yang didelegasikan. Jika Anda mencoba untuk menunjuk beberapa administrator yang didelegasikan di Audit Manager, Anda menerima pesan galat berikut:

- Konsol: You have exceeded the allowed number of delegated administrators for the delegated service
- CLI: An error occurred (ValidationException) when calling the RegisterAccount operation: Cannot change delegated Admin for an active account 11111111111 from 222222222222 to 333333333333

Pilih satu akun individu yang ingin Anda gunakan sebagai administrator yang didelegasikan di Manajer Audit. Pastikan Anda mendaftarkan akun administrator yang didelegasikan di Organisasi terlebih dahulu, lalu [tambahkan akun yang sama dengan administrator yang didelegasikan](#) di Manajer Audit.

Saat membuat penilaian, saya tidak dapat melihat akun dari organisasi saya di bawah Akun dalam cakupan

Jika Anda ingin penilaian Manajer Audit menyertakan beberapa akun dari organisasi Anda, Anda harus menentukan administrator yang didelegasikan.

Pastikan Anda mengonfigurasi akun administrator yang didelegasikan untuk Audit Manager. Untuk petunjuk, lihat [Menambahkan administrator yang didelegasikan](#).

Beberapa masalah yang perlu diingat:

- Anda tidak dapat menggunakan akun AWS Organizations manajemen sebagai administrator yang didelegasikan di Audit Manager.
- Jika Anda ingin mengaktifkan Audit Manager di lebih dari satu Wilayah AWS, Anda harus menetapkan akun administrator yang didelegasikan secara terpisah di setiap Wilayah. Di setelan Audit Manager Anda, tentukan akun administrator yang didelegasikan yang sama di semua Wilayah.
- Saat Anda menunjuk administrator yang didelegasikan, pastikan bahwa akun administrator yang didelegasikan memiliki akses pada kunci KMS yang Anda berikan saat menyiapkan Audit Manager.

Untuk mempelajari cara meninjau dan mengubah pengaturan enkripsi Anda, lihat [Mengkonfigurasi pengaturan enkripsi data Anda](#).

Saya mendapatkan akses ditolak kesalahan saat saya mencoba membuat laporan penilaian menggunakan akun administrator yang didelegasikan

Anda akan mendapatkan `access denied` kesalahan jika penilaian dibuat oleh akun administrator yang didelegasikan yang bukan milik kunci KMS yang ditentukan dalam pengaturan Manajer Audit Anda. Untuk menghindari kesalahan ini, saat Anda menunjuk administrator yang didelegasikan untuk Audit Manager, pastikan bahwa akun administrator yang didelegasikan memiliki akses pada kunci KMS yang Anda berikan saat menyiapkan Audit Manager.

Anda mungkin juga menerima `access denied` kesalahan jika Anda tidak memiliki izin menulis untuk bucket S3 yang Anda gunakan sebagai tujuan laporan penilaian.

Jika Anda mendapatkan `access denied` kesalahan, pastikan Anda memenuhi persyaratan berikut:

- Kunci KMS Anda di setelan Audit Manager memberikan izin kepada administrator yang didelegasikan. Anda dapat mengonfigurasi ini dengan mengikuti petunjuk di [Mengizinkan pengguna di akun lain menggunakan kunci KMS](#) di Panduan Peng AWS Key Management Service embang. Untuk petunjuk tentang cara meninjau dan mengubah pengaturan enkripsi Anda di Audit Manager, lihat [Mengkonfigurasi pengaturan enkripsi data Anda](#).
- Anda memiliki kebijakan izin yang memberi Anda akses menulis untuk tujuan laporan penilaian. Lebih khusus lagi, kebijakan izin berisi `s3:PutObject` tindakan, menentukan ARN bucket S3, dan menyertakan kunci KMS yang digunakan untuk mengenkripsi laporan penilaian Anda. Untuk contoh kebijakan yang dapat Anda gunakan, lihat [Contoh 2 \(Izin tujuan laporan penilaian\)](#).

Note

Jika Anda mengubah setelan enkripsi data Audit Manager, perubahan ini berlaku untuk penilaian baru yang Anda buat di masa mendatang. Ini termasuk laporan penilaian apa pun yang Anda buat dari penilaian baru Anda.

Perubahan tidak berlaku untuk penilaian yang sudah ada yang Anda buat sebelum mengubah setelan enkripsi. Ini termasuk laporan penilaian baru yang Anda buat dari penilaian yang ada, selain laporan penilaian yang ada. Penilaian yang ada — dan semua laporan penilaian mereka — terus menggunakan kunci KMS lama. Jika identitas IAM yang

membuat laporan penilaian tidak memiliki izin untuk menggunakan kunci KMS lama, Anda dapat memberikan izin di tingkat kebijakan utama.

Apa yang terjadi di Audit Manager jika saya memutuskan tautan akun anggota dari organisasi saya?

Saat Anda memutuskan tautan akun anggota dari organisasi, Manajer Audit menerima pemberitahuan tentang acara ini. Audit Manager kemudian secara otomatis menghapus Akun AWS apusnya dari akun dalam daftar lingkup penilaian Anda yang ada. Saat Anda menentukan ruang lingkup penilaian baru ke depan, akun yang tidak ditautkan tidak lagi muncul dalam daftar yang memenuhi syarat Akun AWS.

Saat Manajer Audit menghapus akun anggota yang tidak ditautkan dari akun dalam daftar cakupan penilaian Anda, Anda tidak diberi tahu tentang perubahan ini. Selain itu, akun anggota yang tidak ditautkan tidak diberi tahu bahwa Manajer Audit tidak lagi diaktifkan di akun mereka.

Apa yang terjadi jika saya menautkan ulang akun anggota ke organisasi saya?

Saat Anda menautkan ulang akun anggota ke organisasi, akun tersebut tidak secara otomatis ditambahkan ke cakupan penilaian Manajer Audit yang ada. Namun, akun anggota yang di-link ulang sekarang muncul sebagai memenuhi syarat Akun AWS saat Anda menentukan akun dalam lingkup penilaian Anda.

- Untuk penilaian yang ada, Anda dapat mengedit cakupan penilaian secara manual untuk menambahkan akun anggota yang di-link ulang. Untuk petunjuk, lihat [Langkah 2: Sunting Akun AWS dalam ruang lingkup](#).
- Untuk penilaian baru, Anda dapat menambahkan akun yang di-link ulang selama penyiapan penilaian. Untuk petunjuk, lihat [Langkah 2: Tentukan Akun AWS dalam ruang lingkup](#).

Apa yang terjadi jika saya memigrasikan akun anggota dari satu organisasi ke organisasi lain?

Jika akun anggota mengaktifkan Manajer Audit di organisasi 1 dan kemudian bermigrasi ke organisasi 2, Pengelola Audit tidak diaktifkan untuk organisasi 2 sebagai hasilnya.

Memecahkan masalah pencari bukti

Gunakan informasi di halaman ini untuk menyelesaikan masalah pencari bukti umum di Manajer Audit.

Masalah pencari bukti umum

- [Saya tidak dapat mengaktifkan pencari bukti](#)
- [Saya mengaktifkan pencari bukti, tetapi saya tidak melihat bukti masa lalu di hasil pencarian saya](#)
- [Saya tidak dapat menonaktifkan pencari bukti](#)
- [Kueri pencarian saya gagal](#)
- [Saya melihat bahwa domain kontrol ditandai sebagai “usang”. Apa artinya ini?](#)

Masalah laporan penilaian pencari bukti

- [Saya tidak dapat membuat beberapa laporan penilaian dari hasil pencarian](#)
- [Saya tidak dapat memasukkan bukti spesifik dari hasil pencarian saya](#)
- [Tidak semua hasil pencari bukti saya disertakan dalam laporan penilaian](#)
- [Saya ingin membuat laporan penilaian dari hasil pencarian saya, tetapi pernyataan kueri saya gagal](#)
- [Sumber daya tambahan](#)

Masalah ekspor CSV pencari bukti

- [Ekspor CSV saya gagal](#)
- [Saya tidak dapat mengekspor bukti spesifik dari hasil pencarian saya](#)
- [Saya tidak dapat mengekspor beberapa file CSV sekaligus](#)

Saya tidak dapat mengaktifkan pencari bukti

Alasan umum mengapa Anda tidak dapat mengaktifkan pencari bukti meliputi situasi berikut:

Anda kehilangan izin

Jika Anda mencoba mengaktifkan pencari bukti untuk pertama kalinya, pastikan Anda memiliki izin yang [diperlukan untuk mengaktifkan pencari bukti](#). Izin ini memungkinkan Anda membuat dan mengelola penyimpanan data peristiwa di CloudTrail Lake, yang diperlukan untuk mendukung permintaan pencarian pencari bukti. Izin juga memungkinkan Anda untuk menjalankan kueri pencarian di pencari bukti.

Jika Anda memerlukan bantuan dengan izin, hubungi AWS administrator Anda. Jika Anda seorang AWS administrator, Anda dapat menyalin pernyataan izin yang diperlukan dan [melampirkannya ke kebijakan](#) IAM.

Anda menggunakan akun manajemen Organisasi

Perlu diingat bahwa Anda tidak dapat menggunakan akun manajemen untuk mengaktifkan pencari bukti. Masuk sebagai akun administrator yang didelegasikan, dan coba lagi.

Anda sebelumnya menonaktifkan pencari bukti

Re-enabling Pencari bukti saat ini tidak didukung. Jika sebelumnya Anda menonaktifkan pencari bukti, Anda tidak dapat mengaktifkannya lagi.

Saya mengaktifkan pencari bukti, tetapi saya tidak melihat bukti masa lalu di hasil pencarian saya

Ketika Anda mengaktifkan pencari bukti, dibutuhkan waktu hingga 7 hari agar semua data bukti masa lalu Anda tersedia.

Selama periode 7 hari ini, penyimpanan data acara diisi ulang dengan data bukti dua tahun terakhir Anda. Ini berarti bahwa jika Anda menggunakan pencari bukti segera setelah Anda mengaktifkannya, tidak semua hasil tersedia sampai pengisian ulang selesai.

Untuk petunjuk tentang cara memeriksa status isi ulang data, lihat [Mengkonfirmasi status pencari bukti](#).

Saya tidak dapat menonaktifkan pencari bukti

Ini bisa disebabkan oleh salah satu alasan berikut.

Anda kehilangan izin

Jika Anda mencoba menonaktifkan pencari bukti, pastikan Anda memiliki izin yang [diperlukan untuk menonaktifkan pencari bukti](#). Izin ini memungkinkan Anda memperbarui dan menghapus penyimpanan data peristiwa di CloudTrail Lake, yang diperlukan untuk menonaktifkan pencari bukti.

Jika Anda memerlukan bantuan dengan izin, hubungi AWS administrator Anda. Jika Anda seorang AWS administrator, Anda dapat menyalin pernyataan izin yang diperlukan dan [melampirkannya ke kebijakan](#) IAM.

Permintaan untuk mengaktifkan pencari bukti masih berlangsung

Saat Anda meminta untuk mengaktifkan pencari bukti, kami membuat penyimpanan data peristiwa untuk mendukung kueri pencari bukti. Anda tidak dapat menonaktifkan pencari bukti saat penyimpanan data peristiwa sedang dibuat.

Untuk melanjutkan, tunggu sampai penyimpanan data acara dibuat, dan coba lagi. Untuk informasi selengkapnya, lihat [Mengkonfirmasi status pencari bukti](#).

Anda sudah meminta untuk menonaktifkan pencari bukti

Saat Anda meminta untuk menonaktifkan pencari bukti, kami menghapus penyimpanan data peristiwa yang digunakan untuk kueri pencari bukti. Jika Anda mencoba lagi untuk menonaktifkan pencari bukti saat penyimpanan data peristiwa sedang dihapus, Anda mendapatkan pesan kesalahan.

Dalam hal ini, tidak diperlukan tindakan. Tunggu penyimpanan data acara dihapus. Segera setelah ini selesai, pencari bukti dinonaktifkan. Untuk informasi selengkapnya, lihat [Mengkonfirmasi status pencari bukti](#).

Kueri pencarian saya gagal

Permintaan pencarian yang gagal dapat disebabkan oleh salah satu alasan berikut.

Anda kehilangan izin

Verifikasi bahwa pengguna memiliki izin yang [diperlukan untuk menjalankan kueri penelusuran](#) dan mengakses hasil pencarian. Secara khusus, Anda memerlukan izin untuk CloudTrail tindakan berikut:

- [StartQuery](#)

- [DescribeQuery](#)
- [CancelQuery](#)
- [GetQueryResults](#)

Jika Anda memerlukan bantuan dengan izin, hubungi AWS administrator Anda. Jika Anda seorang AWS administrator, Anda dapat menyalin pernyataan izin yang diperlukan dan [melampirkannya ke kebijakan](#) IAM.

Anda menjalankan jumlah kueri maksimum

Anda dapat menjalankan hingga 5 kueri sekaligus. Jika Anda menjalankan jumlah maksimum kueri bersamaan, ini akan menghasilkan `MaxConcurrentQueriesException` kesalahan. Jika Anda mendapatkan pesan kesalahan ini, tunggu sebentar hingga beberapa kueri selesai, lalu jalankan kueri lagi.

Pernyataan kueri Anda memiliki kesalahan validasi

Jika Anda menggunakan API atau CLI untuk melakukan [StartQuery](#) operasi CloudTrail Lake, pastikan bahwa Anda `queryStatement` valid. Jika pernyataan kueri memiliki kesalahan validasi, sintaks yang salah, atau kata kunci yang tidak didukung, ini menghasilkan `InvalidQueryStatementException`

Untuk informasi selengkapnya tentang menulis kueri, lihat [Membuat atau mengedit kueri](#) di Panduan AWS CloudTrail Pengguna.

Untuk contoh sintaks yang valid, tinjau contoh pernyataan kueri berikut yang dapat digunakan untuk menanyakan penyimpanan data peristiwa Audit Manager.

Contoh 1: Selidiki bukti dan status kepatuhannya

Contoh ini menemukan bukti dengan status kepatuhan apa pun di semua penilaian dalam akun, dalam rentang tanggal tertentu.

```
SELECT eventData.evidenceId, eventData.resourceArn,  
       eventData.resourceComplianceCheck FROM $EDS_ID WHERE eventTime > '2022-11-02  
00:00:00.000' AND eventTime < '2022-11-03 00:00:00.000'
```

Contoh 2: Tentukan bukti yang tidak sesuai untuk kontrol

Contoh ini menemukan semua bukti yang tidak sesuai dalam rentang tanggal tertentu untuk penilaian dan kontrol tertentu.


```
SELECT * FROM $EDS_ID WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime > '2022-10-27 22:05:00.000' AND eventTime < '2022-11-03 22:05:00.000' AND eventData.resourceComplianceCheck IN ('NON_COMPLIANT', 'FAILED', 'WARNING') AND eventData.controlId IN ('aa11bb22-cc33-dd44-ee55-ff66gg77hh88')
```

Contoh 3: Hitung bukti berdasarkan nama

Contoh ini mencantumkan bukti total untuk penilaian dalam rentang tanggal tertentu, dikelompokkan berdasarkan nama dan diurutkan berdasarkan jumlah bukti.

```
SELECT eventData.eventName as eventName, COUNT(*) as totalEvidence FROM $EDS_ID WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime > '2022-10-27 22:05:00.000' AND eventTime < '2022-11-03 22:05:00.000' GROUP BY eventData.eventName ORDER BY totalEvidence DESC
```

Contoh 4: Jelajahi bukti berdasarkan sumber data dan layanan

Contoh ini menemukan semua bukti dalam rentang tanggal tertentu untuk sumber dan layanan data tertentu.

```
SELECT * FROM $EDS_ID WHERE eventTime > '2022-10-27 22:05:00.000' AND eventTime < '2022-11-03 22:05:00.000' AND eventData.service IN ('dynamodb') AND eventData.dataSource IN ('AWS API calls')
```

Contoh 5: Jelajahi bukti yang sesuai berdasarkan sumber data dan domain kontrol

Contoh ini menemukan bukti yang sesuai untuk domain kontrol tertentu, di mana bukti berasal dari sumber data yang bukan AWS Config.

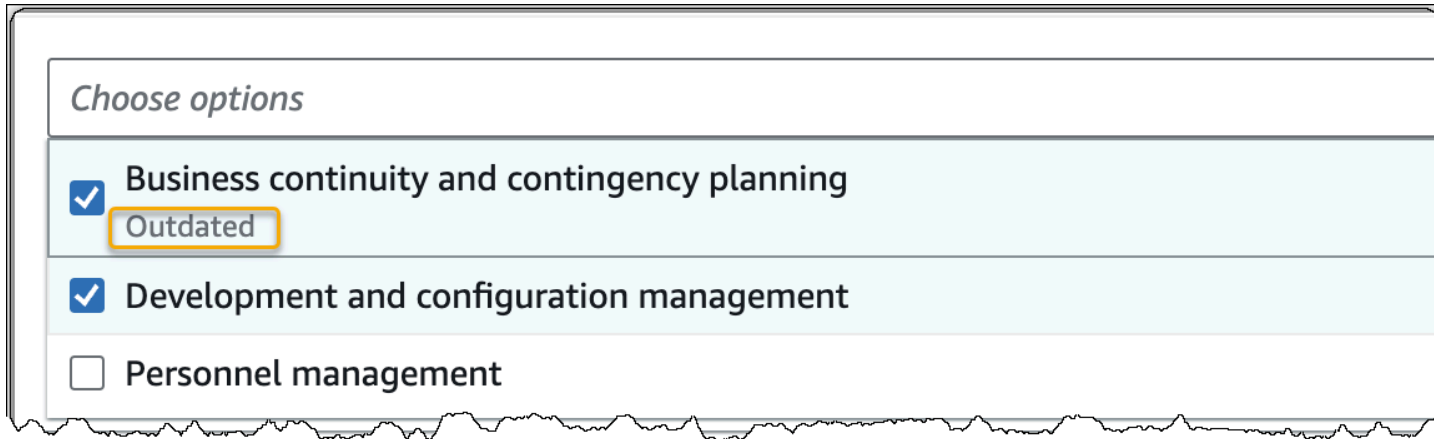
```
SELECT * FROM $EDS_ID WHERE eventData.resourceComplianceCheck IN ('PASSED', 'COMPLIANT') AND eventData.controlDomainName IN ('Logging and monitoring', 'Data security and privacy') AND eventData.dataSource NOT IN ('AWS Config')
```

Pengecualian API lainnya

[StartQuery](#) API mungkin gagal karena beberapa alasan lain. Untuk daftar lengkap kemungkinan kesalahan dan deskripsi, lihat Kes [StartQuery alahan](#) dalam Referensi AWS CloudTrail API.

Saya melihat bahwa domain kontrol ditandai sebagai “usang”. Apa artinya ini?

Saat Anda menerapkan filter domain kontrol di pencari bukti, Anda mungkin memperhatikan bahwa beberapa domain kontrol yang tersedia digambarkan sebagai Kedaluwarsa.



Choose options

- ☒ Business continuity and contingency planning
Outdated
- ☒ Development and configuration management
- ☐ Personnel management

Mulai 6 Juni 2024, Manajer Audit mendukung serangkaian domain kontrol baru yang disediakan oleh Katalog AWS Kontrol. Untuk mengambil daftar domain kontrol ini, lihat [ListDomains](#) di Referensi API Katalog AWS Kontrol.

Jika domain kontrol ditandai sebagai Kedaluwarsa, ini berarti domain kontrol yang Anda lihat bukan salah satu domain kontrol baru yang disediakan oleh Katalog AWS Kontrol. Audit Manager terus mendukung domain kontrol yang sudah ketinggalan zaman ini sehingga Anda masih dapat menggunakannya sebagai kriteria saat Anda mencari bukti.

Meskipun kami terus mendukung domain kontrol yang sudah ketinggalan zaman, kami menyarankan Anda untuk menggunakan domain kontrol baru sebagai gantinya. Domain kontrol baru dipetakan ke kontrol standar yang diperbarui yang diluncurkan sebagai bagian dari pustaka kontrol umum pada 6 Juni 2024. Pada tanggal ini, kami merilis kontrol standar yang diperbarui yang dapat mengumpulkan bukti dari sumber [AWS terkelola](#). Ini berarti bahwa setiap kali ada pembaruan ke sumber data yang mendasari untuk kontrol umum atau inti, Audit Manager secara otomatis menerapkan pembaruan yang sama ke semua kontrol standar terkait.

Saya tidak dapat membuat beberapa laporan penilaian dari hasil pencarian

Kesalahan ini disebabkan oleh menjalankan terlalu banyak kueri CloudTrail Lake secara bersamaan.

Kesalahan ini dapat terjadi jika Anda mengelompokkan hasil pencarian dan mencoba untuk segera membuat laporan penilaian untuk setiap item baris dalam hasil yang dikelompokkan. Ketika Anda

mendapatkan hasil pencarian dan membuat laporan penilaian, setiap tindakan akan memanggil kueri. Anda hanya dapat menjalankan hingga 5 kueri sekaligus. Jika Anda menjalankan jumlah maksimum kueri bersamaan, `MaxConcurrentQueriesException` kesalahan dikembalikan.

Untuk mencegah kesalahan ini, pastikan Anda tidak menghasilkan terlalu banyak laporan penilaian sekaligus. Jika Anda menjalankan jumlah maksimum kueri bersamaan, `MaxConcurrentQueriesException` kesalahan dikembalikan. Jika Anda mendapatkan pesan kesalahan ini, tunggu beberapa menit hingga laporan penilaian yang sedang berjalan selesai.

Anda dapat memeriksa status laporan penilaian Anda dari halaman pusat unduhan di konsol Audit Manager. Setelah laporan Anda selesai, kembali ke hasil yang dikelompokkan di pencari bukti. Anda kemudian dapat terus mendapatkan hasil dan menghasilkan laporan penilaian untuk setiap item baris.

Saya tidak dapat memasukkan bukti spesifik dari hasil pencarian saya

Semua hasil pencarian Anda disertakan dalam laporan penilaian. Anda tidak dapat secara selektif menambahkan baris individual dari kumpulan hasil pencarian Anda.

Jika Anda hanya ingin menyertakan hasil penelusuran tertentu dalam laporan penilaian, sebaiknya [edit filter penelusuran saat ini](#). Dengan cara ini, Anda dapat mempersempit hasil Anda untuk menargetkan hanya bukti yang ingin Anda sertakan dalam laporan.

Tidak semua hasil pencari bukti saya disertakan dalam laporan penilaian

Ketika Anda membuat laporan penilaian, ada batasan untuk berapa banyak bukti yang dapat Anda tambahkan. Batas didasarkan pada Wilayah AWS penilaian Anda, Wilayah bucket S3 yang digunakan sebagai tujuan laporan penilaian Anda, dan apakah penilaian Anda menggunakan pengelolaan pelanggan AWS KMS key.

1. Batasnya adalah 22.000 untuk laporan wilayah yang sama (di mana bucket S3 dan penilaian berada di tempat yang sama) Wilayah AWS
2. Batasnya adalah 3.500 untuk laporan lintas wilayah (di mana bucket S3 dan penilaian berbeda) Wilayah AWS
3. Batasnya adalah 3.500 jika penilaian menggunakan kunci KMS yang dikelola pelanggan

Jika Anda melebihi batas ini, laporan masih dibuat. Namun, Audit Manager hanya menambahkan 3.500 atau 22.000 item bukti pertama ke dalam laporan.

Untuk mencegah masalah ini, kami sarankan Anda [mengedit filter pencarian Anda saat ini](#). Dengan cara ini, Anda dapat mengurangi hasil pencarian Anda dengan menargetkan jumlah bukti yang lebih kecil. Jika perlu, Anda dapat mengulangi metode ini dan menghasilkan beberapa laporan penilaian alih-alih satu laporan yang lebih besar.

Saya ingin membuat laporan penilaian dari hasil pencarian saya, tetapi pernyataan kueri saya gagal

Jika Anda menggunakan [CreateAssessmentReport](#) API dan pernyataan kueri Anda mengembalikan pengecualian validasi, periksa tabel di bawah ini untuk panduan tentang cara memperbaikinya.

Note

Bahkan jika pernyataan kueri berfungsi CloudTrail, kueri yang sama mungkin tidak valid untuk pembuatan laporan penilaian di Audit Manager. Ini karena beberapa perbedaan dalam validasi kueri antara kedua layanan.

Klausul	Isu	Solusi	Catatan
SELECT	Kla SELECT usa berisi nama kolom	Hapus SELECT klausa dan ganti dengan <code>SELECT eventJson</code> .	Hanya <code>SELECT eventJson</code> didukung. Validasi ini ditangani oleh Audit Manager.
FROM	Kla FROM usa berisi ID penyimpanan data peristiwa yang tidak valid atau ID penyimpanan data peristiwa yang disediakan tidak cocok dengan ID penyimpanan data	Hapus FROM klausa dan ganti dengan <code>FROM edsID</code> , di mana nilai <code>edsID</code> cocok dengan ID penyimpanan data peristiwa yang ditentukan dalam pengaturan Manajer Audit Anda. Anda dapat mengambil ARN dari penyimpanan data peristiwa dari pengaturan Audit Manager Anda. Untuk informasi selengkapnya, lihat GetSettin	Validasi ini ditangani oleh Audit Manager.

Klausul	Isu	Solusi	Catatan
	peristiwa di setelan Audit Manager Anda	gs di dalam Referensi API AWS Audit Manager .	
GROUP BY	Sebuah GROUP BY klausa hadir dalam query	Hapus GROUP BY klausa.	Validasi ini ditangani oleh Audit Manager.
HAVING	Sebuah HAVING klausa hadir dalam query	Hapus HAVING klausa.	Validasi ini ditangani oleh Audit Manager.
LIMIT	Kla LIMIT usa berisi nilai yang melebihi batas maksimum yang diizinkan	Jika LIMIT klausa ada, pastikan nilainya sama dengan atau kurang dari batas maksimum yang didukung: • Untuk laporan wilayah yang sama, batasnya adalah 22.000 • Untuk laporan lintas wilayah, batasnya adalah 3.500 • Untuk laporan di mana penilaian terkait menggunakan pengelolaan pelanggan AWS KMS key, batasnya adalah 3.500	Di konsol, tidak ada batasan jumlah hasil bukti yang dapat dikembalikan. Namun, saat membuat laporan penilaian , batas berlaku untuk jumlah bukti yang dapat Anda sertakan. Jika tidak ada LIMIT nilai yang diberikan dalam pernyataan kueri Anda, batas maksimum default diterapkan. Validasi ini ditangani oleh Audit Manager.
ORDER BY	Kla ORDER BY usa berisi fungsi Agregat atau Alias yang tidak ada dalam klausa SELECT	Pastikan ORDER BY klausa tidak mengandung kondisi apa pun menggunakan fungsi Agregat atau Alias.	Validasi ini ditangani oleh CloudTrail StartQuery API .

Klausul	Isu	Solusi	Catatan
WHERE	K WHERE lausul berisi lebih dari satu assessmentId atau Kla WHERE usa berisi sebuah assessmentId yang tidak cocok assessmentId dengan createAssessmentReport permintaan Anda atau Kla WHERE usa berisi nama kolom yang tidak didukung	Pastikan hanya satu Assessment tID yang ditentukan, dan cocok dengan parameter Assessmen tID yang Anda tentukan dalam permintaan API. createAssessmentReport Hapus nama kolom yang tidak didukung.	Validasi ini ditangani oleh CloudTrail StartQuery API .

Contoh

Contoh berikut menunjukkan bagaimana Anda dapat menggunakan queryStatement parameter saat memanggil [CreateAssessmentReport](#) operasi. Sebelum Anda menggunakan kueri ini, ganti *placeholder text* dengan assessmentId nilai Anda sendiri dsId.

Contoh 1: Buat laporan (Batas wilayah yang sama berlaku)

Contoh ini membuat laporan yang menyertakan hasil untuk bucket S3 yang dibuat antara 22-23 Januari 2022.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime > '2022-01-22 00:00:00.000' AND eventTime < '2022-01-23 00:00:00.000' AND eventName='CreateBucket' LIMIT 22000
```

Contoh 2: Buat laporan (Batas lintas wilayah berlaku)

Contoh ini membuat laporan yang mencakup semua hasil untuk penyimpanan dan penilaian data peristiwa tertentu, tanpa rentang tanggal yang ditentukan.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 7000
```

Contoh 3: Buat laporan (di bawah batas default)

Contoh ini membuat laporan yang mencakup semua hasil untuk penyimpanan dan penilaian data peristiwa tertentu, dengan batas yang berada di bawah maksimum default.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 2000
```

Sumber daya tambahan

Halaman berikut berisi panduan pemecahan masalah umum tentang laporan penilaian:

- [Memecahkan masalah laporan penilaian](#)

Ekspor CSV saya gagal

Ekspor CSV Anda mungkin gagal karena beberapa alasan. Anda dapat memecahkan masalah ini dengan memeriksa penyebab yang paling sering.

Pertama, pastikan Anda memenuhi prasyarat untuk menggunakan fitur ekspor CSV:

Anda berhasil mengaktifkan pencari bukti

Jika belum [mengaktifkan pencari bukti](#), Anda tidak dapat menjalankan kueri penelusuran dan mengekspor hasil pencarian Anda.

Pengisian ulang penyimpanan data acara Anda selesai

Jika Anda menggunakan pencari bukti segera setelah Anda mengaktifkannya, dan pengisian [ulang](#) bukti masih berlangsung, mungkin ada beberapa hasil yang tidak tersedia. Untuk memeriksa status isi ulang, lihat [Mengkonfirmasi status pencari bukti](#).

Kueri penelusuran Anda berhasil

Audit Manager tidak dapat mengekspor hasil kueri yang gagal. Untuk memecahkan masalah kueri yang gagal, lihat [Kueri pencarian saya gagal](#).

Setelah Anda mengonfirmasi bahwa Anda memenuhi prasyarat, gunakan daftar periksa berikut untuk memeriksa potensi masalah:

1. Periksa status permintaan pencarian Anda:

- a. Apakah kueri dibatalkan? Pencari bukti menampilkan sebagian hasil yang diproses sebelum kueri dibatalkan. Namun, Audit Manager tidak mengeksport hasil paruh ke bucket S3 atau pusat unduhan.
- b. Apakah kueri berjalan selama lebih dari satu jam? Kueri yang berjalan lebih dari satu jam mungkin habis. Pencari bukti menampilkan sebagian hasil yang diproses sebelum waktu kueri habis. Namun, Audit Manager tidak mengeksport hasil paruh. Untuk menghindari batas waktu, Anda dapat mengurangi jumlah bukti yang dipindai [Mengedit filter pencarian](#) untuk menentukan rentang waktu yang lebih sempit.

2. Periksa nama dan URI bucket S3 tujuan ekspor Anda:

- a. Apakah bucket yang Anda tentukan ada? Jika Anda memasukkan URI bucket secara manual, pastikan Anda tidak salah mengetik apa pun. Salah ketik atau URI yang salah dapat mengakibatkan RESOURCE_NOT_FOUND kesalahan saat Audit Manager mencoba mengeksport file CSV ke Amazon S3.

3. Periksa izin bucket S3 tujuan ekspor Anda:

- a. Apakah Anda memiliki izin menulis untuk bucket S3? Anda harus memiliki akses tulis untuk bucket S3 yang Anda gunakan sebagai tujuan ekspor. Lebih khusus lagi, kebijakan izin IAM harus menyertakan `s3:PutObject` tindakan dan bucket ARN, dan daftar CloudTrail sebagai prinsipal layanan. Kami memberikan [contoh kebijakan](#) yang dapat Anda gunakan.

4. Periksa apakah ada Wilayah AWS informasi Anda yang tidak cocok:

- a. Apakah kunci Wilayah AWS yang dikelola pelanggan Anda cocok Wilayah AWS dengan penilaian Anda? Jika Anda memberikan kunci yang dikelola pelanggan untuk enkripsi data, kunci tersebut harus Wilayah AWS sama dengan penilaian Anda. Untuk petunjuk tentang cara mengubah kunci KMS, lihat [Mengkonfigurasi pengaturan enkripsi data Anda](#).

5. Periksa izin akun administrator yang didelegasikan:

- a. Apakah kunci yang dikelola pelanggan di setelan Audit Manager memberikan izin kepada administrator yang didelegasikan? Jika Anda menggunakan akun administrator yang didelegasikan dan Anda menentukan kunci yang dikelola pelanggan untuk enkripsi data, pastikan administrator yang didelegasikan memiliki akses pada kunci KMS tersebut. Untuk petunjuk, lihat [Mengizinkan pengguna di akun lain menggunakan kunci KMS](#) di Panduan Peng AWS Key Management Service embang. Untuk meninjau dan mengubah pengaturan enkripsi Anda di Audit Manager, lihat [Mengkonfigurasi pengaturan enkripsi data Anda](#).

 Note

Jika Anda mengubah setelan enkripsi data Audit Manager, perubahan ini berlaku untuk penilaian baru yang Anda buat di masa mendatang. Ini termasuk file CSV apa pun yang Anda ekspor dari penilaian baru Anda.

Perubahan tidak berlaku untuk penilaian yang sudah ada yang Anda buat sebelum mengubah setelan enkripsi. Ini termasuk ekspor CSV baru dari penilaian yang ada, selain ekspor CSV yang ada. Penilaian yang ada—dan semua ekspor CSV-nya—terus menggunakan kunci KMS lama. Jika identitas IAM yang mengekspor file CSV tidak memiliki izin untuk menggunakan kunci KMS lama, Anda dapat memberikan izin di tingkat kebijakan utama.

Saya tidak dapat mengekspor bukti spesifik dari hasil pencarian saya

Semua hasil pencarian Anda disertakan dalam hasil.

Jika Anda hanya ingin menyertakan bukti tertentu dalam file CSV, sebaiknya [edit filter penelusuran saat ini](#). Dengan cara ini, Anda dapat mempersempit hasil untuk menargetkan hanya bukti yang ingin Anda ekspor.

Saya tidak dapat mengekspor beberapa file CSV sekaligus

Kesalahan ini disebabkan oleh menjalankan terlalu banyak kueri CloudTrail Lake secara bersamaan.

Hal ini dapat terjadi jika Anda mengelompokkan hasil pencarian dan mencoba untuk segera mengekspor file CSV untuk setiap item baris dalam hasil yang dikelompokkan. Saat Anda mendapatkan hasil pencarian dan mengekspor file CSV, setiap tindakan ini akan memanggil kueri. Anda hanya dapat menjalankan hingga lima kueri sekaligus. Jika Anda menjalankan jumlah maksimum kueri bersamaan, `MaxConcurrentQueriesException` kesalahan dikembalikan.

Untuk mencegah kesalahan ini, pastikan Anda tidak mengekspor terlalu banyak file CSV sekaligus.

Untuk mengatasi kesalahan ini, tunggu hingga ekspor CSV Anda yang sedang berlangsung selesai. Sebagian besar ekspor membutuhkan waktu beberapa menit. Namun, jika Anda mengekspor data dalam jumlah yang sangat besar, mungkin diperlukan waktu hingga satu jam untuk menyelesaikan ekspor. Jangan ragu untuk menavigasi jauh dari pencari bukti saat ekspor sedang berlangsung.

Anda dapat memeriksa status ekspor dari pusat unduhan di konsol Audit Manager. Setelah file yang diekspor siap, kembali ke hasil yang dikelompokkan di pencari bukti. Anda kemudian dapat terus mendapatkan hasil dan mengekspor file CSV untuk setiap item baris.

Memecahkan masalah kerangka kerja

Anda dapat menggunakan informasi di halaman ini untuk menyelesaikan masalah kerangka kerja umum di Audit Manager.

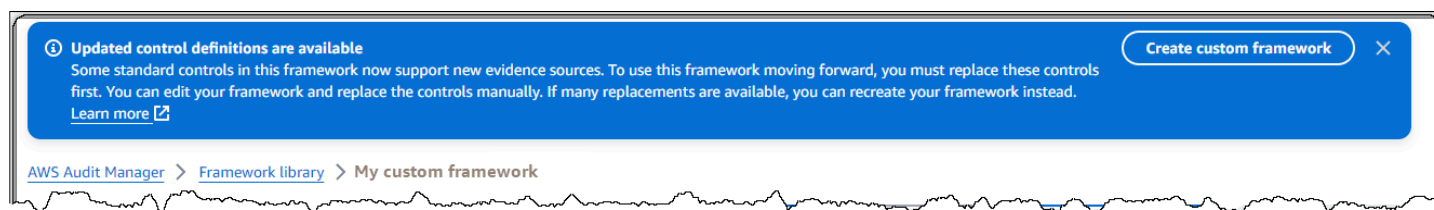
Masalah kerangka kerja umum

- [Pada halaman detail kerangka kerja kustom saya, saya diminta untuk membuat ulang kerangka kerja khusus saya](#)
- [Saya tidak dapat membuat salinan kerangka kerja khusus saya](#)

Masalah berbagi kerangka kerja

- [Status permintaan berbagi yang saya kirim ditampilkan sebagai Gagal](#)
- [Permintaan berbagi saya memiliki titik biru di sebelahnya. Apa artinya ini?](#)
- [Kerangka kerja bersama saya memiliki kontrol yang menggunakan kustom AWS Config aturan sebagai sumber data. Dapatkah penerima mengumpulkan bukti untuk kontrol ini?](#)
- [Saya memperbarui aturan khusus yang digunakan dalam kerangka kerja bersama. Apakah saya perlu mengambil tindakan apa pun?](#)

Pada halaman detail kerangka kerja kustom saya, saya diminta untuk membuat ulang kerangka kerja khusus saya



Jika Anda melihat pesan yang mengatakan Definisi kontrol yang diperbarui tersedia, ini menunjukkan bahwa Manajer Audit sekarang menyediakan definisi yang lebih baru untuk beberapa kontrol standar yang ada dalam kerangka kustom Anda.

Kontrol standar sekarang dapat mengumpulkan bukti dari [AWS managed source](#). Ini berarti bahwa setiap kali Audit Manager memperbarui sumber data yang mendasari untuk kontrol umum atau inti, pembaruan yang sama secara otomatis diterapkan ke kontrol standar terkait. Ini membantu Anda memastikan kepatuhan berkelanjutan saat lingkungan kepatuhan cloud berubah. Untuk memastikan Anda mendapatkan manfaat dari sumber ter AWS kelola ini, sebaiknya ganti kontrol dalam kerangka kerja kustom Anda.

Dalam kerangka kerja kustom Anda, Audit Manager menunjukkan kontrol mana yang memiliki penggantian yang tersedia. Anda harus mengganti kontrol ini sebelum Anda dapat membuat salinan kerangka kerja kustom Anda. Lain kali Anda mengedit kerangka kerja khusus, kami akan meminta Anda untuk mengganti kontrol ini bersama dengan pengeditan lain yang ingin Anda buat.

Ada dua cara untuk mengganti kontrol dalam kerangka kustom Anda:

1. Buat ulang kerangka kustom Anda

Jika sejumlah besar kontrol memiliki penggantian yang tersedia, sebaiknya buat ulang kerangka kerja kustom Anda. Ini kemungkinan akan menjadi pilihan terbaik jika kerangka kerja kustom Anda didasarkan pada kerangka kerja standar.

- Misalnya, katakanlah Anda membuat kerangka kerja khusus Anda menggunakan [NIST SP 800-53 Rev 5](#) sebagai titik awal. Kerangka kerja standar ini memiliki 1007 kontrol standar, dan Anda menambahkan 20 kontrol khusus.
- Dalam hal ini, opsi yang paling efisien adalah menemukan NIST 800-53 (Rev. 5) Low-Moderate-High di perpustakaan kerangka kerja dan [membuat salinan kerangka](#) kerja yang dapat diedit. Selama proses ini, Anda dapat menambahkan 20 kontrol kustom yang sama yang Anda gunakan sebelumnya. Karena Anda sekarang menggunakan definisi terbaru dari kerangka kerja standar sebagai titik awal Anda, kerangka kerja kustom Anda secara otomatis mewarisi definisi terbaru untuk semua kontrol standar 1007.

2. Mengedit kerangka kerja kustom Anda

Jika sejumlah kecil kontrol memiliki penggantian yang tersedia, kami sarankan Anda mengedit kerangka kerja khusus dan mengganti kontrol secara manual.

- Misalnya, katakanlah Anda membuat kerangka kerja khusus Anda dari awal. Dalam kerangka kustom Anda, Anda menambahkan 20 kontrol khusus yang Anda buat sendiri, dan delapan kontrol standar dari kerangka [ACSC Essential Delapan](#) standar.

- Dalam hal ini, karena maksimal delapan kontrol akan memiliki pembaruan yang tersedia, opsi yang paling efisien adalah mengedit kerangka kerja khusus Anda dan mengganti kontrol tersebut satu per satu. Untuk instruksi, lihat prosedur berikut.

Untuk mengganti kontrol secara manual dalam kerangka kerja kustom Anda

Untuk mengganti kontrol secara manual dalam kerangka kerja kustom Anda

1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Di panel navigasi kiri, pilih pustaka Framework, lalu pilih tab Kerangka kerja khusus.
3. Pilih kerangka kerja yang ingin Anda edit, pilih Tindakan, lalu pilih Edit.
4. Pada halaman detail Edit kerangka kerja, pilih Berikutnya.
5. Pada halaman Edit kumpulan kontrol, tinjau nama setiap kumpulan kontrol untuk melihat apakah ada kontrolnya yang memiliki penggantian yang tersedia.
6. Pilih kumpulan kontrol yang terpengaruh untuk mengembangkannya dan mengidentifikasi kontrol mana yang perlu diganti.

 Tip

Untuk mengidentifikasi kontrol dengan lebih cepat, masukkan **Replacement available** di kotak pencarian.

7. Hapus kontrol yang terpengaruh dengan memilih kotak centang dan memilih Hapus dari kumpulan kontrol.
8. Re-add kontrol yang sama. Tindakan ini menggantikan kontrol yang baru saja Anda hapus dengan definisi kontrol terbaru.
 - a. Di bawah Tambah kontrol, gunakan daftar tarik-turun Jenis kontrol dan pilih Kontrol standar.
 - b. Temukan pengganti untuk kontrol yang baru saja Anda hapus.

 Tip

Dalam beberapa kasus, nama kontrol pengganti mungkin tidak persis sama dengan aslinya. Dalam hal ini, nama kontrol pengganti kemungkinan akan sangat mirip dengan aslinya. Dalam kasus yang jarang terjadi, satu kontrol mungkin diganti dengan dua kontrol (atau sebaliknya).

Jika Anda tidak dapat menemukan kontrol pengganti, kami sarankan Anda melakukan pencarian sebagian. Untuk melakukan ini, masukkan bagian dari nama kontrol asli atau kata kunci yang mewakili apa yang Anda cari. Anda juga dapat mencari berdasarkan jenis kepatuhan untuk lebih mempersempit daftar hasil.

- c. Pilih kotak centang di sebelah kontrol dan pilih Tambahkan ke kumpulan kontrol.
 - d. Di jendela pop-up yang muncul, pilih Tambah untuk mengonfirmasi.
9. Ulangi langkah 6-8 sesuai kebutuhan sampai Anda mengganti semua kontrol.
 10. Pilih Berikutnya.
 11. Pada halaman Tinjau dan simpan, pilih Simpan perubahan.

Saya tidak dapat membuat salinan kerangka kerja khusus saya

Jika tombol Buat salin tidak tersedia di halaman detail kerangka kerja, ini berarti Anda perlu mengganti beberapa kontrol dalam kerangka kustom Anda.

Untuk petunjuk tentang cara melanjutkan, lihat [Pada halaman detail kerangka kerja kustom saya, saya diminta untuk membuat ulang kerangka kerja khusus saya](#).

Status permintaan berbagi yang saya kirim ditampilkan sebagai Gagal

Jika Anda mencoba berbagi kerangka kerja khusus dan operasi gagal, sebaiknya periksa hal berikut:

1. Pastikan Audit Manager diaktifkan di penerima Akun AWS dan di Wilayah yang ditentukan. Untuk daftar Wilayah yang didukung AWS Audit Manager, lihat [AWS Audit Manager titik akhir dan kuota](#) di Referensi Umum Layanan Web Amazon.
2. Pastikan Anda memasukkan Akun AWS ID yang benar ketika Anda menentukan akun penerima.
3. Pastikan Anda tidak menentukan akun AWS Organizations manajemen sebagai penerima. Anda dapat berbagi kerangka kerja khusus dengan administrator yang didelegasikan, tetapi jika Anda mencoba berbagi kerangka kerja khusus dengan akun manajemen, operasi gagal.
4. Jika Anda menggunakan kunci yang dikelola pelanggan untuk mengenkripsi data Manajer Audit Anda, pastikan kunci KMS Anda diaktifkan. Jika kunci KMS dinonaktifkan dan Anda mencoba berbagi kerangka kerja khusus, operasi gagal. Untuk petunjuk tentang cara mengaktifkan kunci KMS yang dinonaktifkan, lihat Meng [aktifkan dan menonaktifkan kunci](#) di Panduan Peng AWS Key Management Service embang.

Permintaan berbagi saya memiliki titik biru di sebelahnya. Apa artinya ini?

Notifikasi titik biru menunjukkan bahwa permintaan berbagi membutuhkan perhatian Anda.

Pemberitahuan titik biru untuk pengirim

Titik pemberitahuan biru muncul di sebelah permintaan berbagi yang dikirim dengan status Kedaluwarsa. Audit Manager menampilkan notifikasi titik biru sehingga Anda dapat mengingatkan penerima untuk mengambil tindakan pada permintaan berbagi sebelum kedaluwarsa.

Agar titik notifikasi biru menghilang, penerima harus menerima atau menolak permintaan. Titik biru juga menghilang jika Anda mencabut permintaan berbagi.

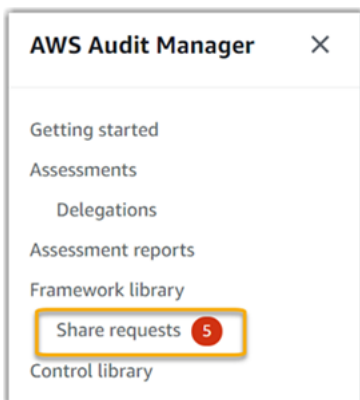
Anda dapat menggunakan prosedur berikut untuk memeriksa permintaan berbagi yang kedaluwarsa, dan mengirim pengingat opsional kepada penerima untuk mengambil tindakan.

Untuk melihat notifikasi untuk permintaan terkirim

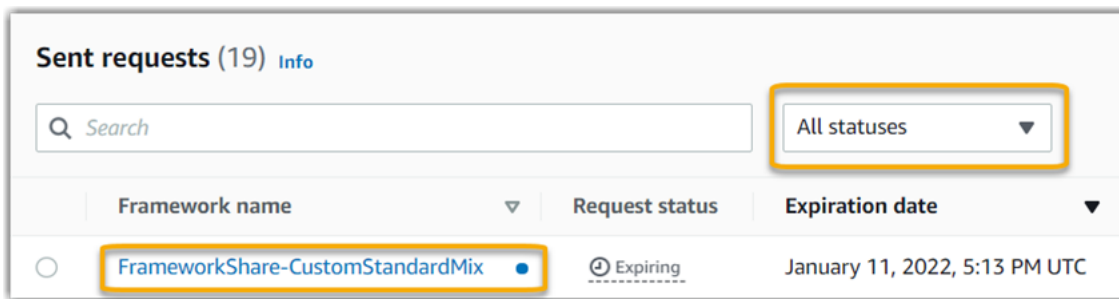
1. Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
2. Jika Anda memiliki pemberitahuan permintaan berbagi, Audit Manager menampilkan titik merah di sebelah ikon menu navigasi.



3. Perluas panel navigasi dan lihat di sebelah Bagikan permintaan. Lencana notifikasi menunjukkan jumlah permintaan berbagi yang perlu diperhatikan.



4. Pilih Bagikan permintaan, lalu pilih tab Per permintaan terkirim.
5. Cari titik biru untuk mengidentifikasi permintaan berbagi yang kedaluwarsa dalam 30 hari ke depan. Atau, Anda juga dapat melihat permintaan berbagi yang kedaluwarsa dengan memilih Kedaluwarsa dari tarik-turun filter Semua status.



- (Optional) Ingatkan penerima bahwa mereka perlu mengambil tindakan atas permintaan berbagi sebelum kedaluwarsa. Langkah ini opsional, karena Audit Manager mengirimkan pemberitahuan di konsol untuk memberi tahu penerima ketika permintaan berbagi aktif atau kedaluwarsa. Namun, Anda juga dapat mengirim pengingat Anda sendiri kepada penerima menggunakan saluran komunikasi pilihan Anda.

Pemberitahuan titik biru untuk penerima

Titik pemberitahuan biru muncul di sebelah permintaan berbagi yang diterima dengan status Aktif atau Kedaluwarsa. Audit Manager menampilkan notifikasi titik biru untuk mengingatkan Anda untuk mengambil tindakan pada permintaan berbagi sebelum kedaluwarsa. Agar titik pemberitahuan biru menghilang, Anda harus menerima atau menolak permintaan. Titik biru juga menghilang jika pengirim mencabut permintaan berbagi.

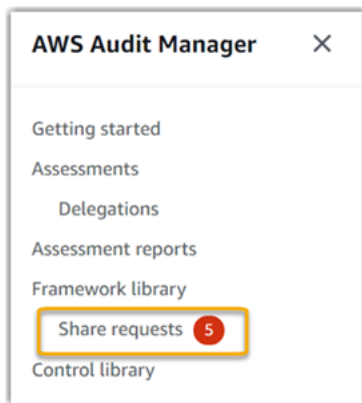
Anda dapat menggunakan prosedur berikut untuk memeriksa permintaan berbagi aktif dan kedaluwarsa.

Untuk melihat notifikasi untuk permintaan yang diterima

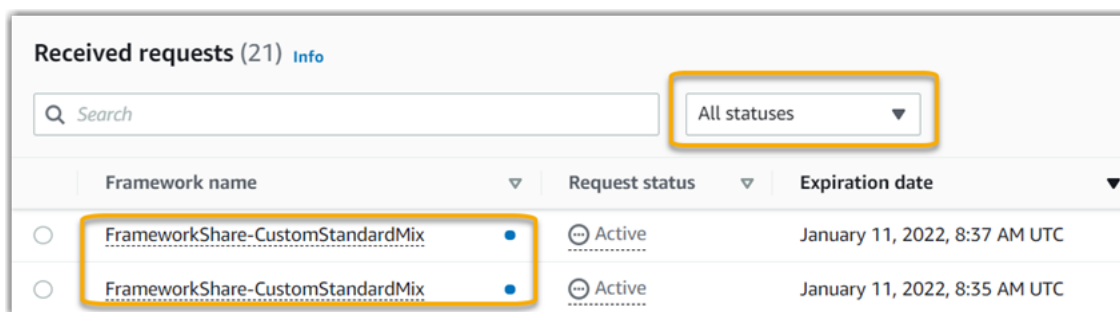
- Buka konsol AWS Audit Manager di <https://console.aws.amazon.com/auditmanager/home>.
- Jika Anda memiliki pemberitahuan permintaan berbagi, Audit Manager menampilkan titik merah di sebelah ikon menu navigasi.



- Perluas panel navigasi dan lihat di sebelah Bagikan permintaan. Lencana notifikasi menunjukkan jumlah permintaan berbagi yang perlu Anda perhatikan.



4. Pilih Bagikan permintaan. Secara default, halaman ini terbuka di tab Per mintaan yang diterima.
5. Identifikasi permintaan berbagi yang memerlukan tindakan Anda dengan mencari item dengan titik biru.



6. (Opsional) Untuk melihat hanya permintaan yang kedaluwarsa dalam 30 hari ke depan, cari daftar dropdown Semua status dan pilih Kedaluwarsa.

Kerangka kerja bersama saya memiliki kontrol yang menggunakan kustom AWS Config aturan sebagai sumber data. Dapatkah penerima mengumpulkan bukti untuk kontrol ini?

Ya, penerima Anda dapat mengumpulkan bukti untuk kontrol ini, tetapi beberapa langkah diperlukan untuk mencapai ini.

Agar Manajer Audit mengumpulkan bukti menggunakan AWS Config aturan sebagai pemetaan sumber data, berikut ini harus benar. Kriteria ini berlaku untuk aturan terkelola dan aturan khusus.

- Aturan harus ada di AWS lingkungan penerima.
- Aturan harus diaktifkan di AWS lingkungan penerima.

Ingatlah bahwa AWS Config aturan di akun Anda mungkin belum ada di AWS lingkungan penerima. Selain itu, ketika penerima menerima permintaan berbagi, Audit Manager tidak membuat ulang aturan khusus apa pun di akun mereka. Agar penerima dapat mengumpulkan bukti menggunakan aturan kustom Anda sebagai pemetaan sumber data, mereka harus membuat aturan khusus yang sama di instans mereka AWS Config. Setelah penerima membuat https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_develop-rules_nodejs.html dan kemudian [mengaktifkan](#) aturan AWS Config, Audit Manager dapat mengumpulkan bukti dari sumber data tersebut.

Sebaiknya Anda berkomunikasi dengan penerima untuk memberi tahu mereka jika ada AWS Config aturan khusus yang harus dibuat dalam instans mereka AWS Config.

Saya memperbarui aturan khusus yang digunakan dalam kerangka kerja bersama. Apakah saya perlu mengambil tindakan apa pun?

Untuk pembaruan aturan dalam AWS lingkungan

Saat Anda memperbarui aturan khusus dalam AWS lingkungan Anda, tidak ada tindakan yang diperlukan di Manajer Audit. Audit Manager mendeteksi dan menangani pembaruan aturan dengan cara yang dijelaskan dalam tabel berikut. Audit Manager tidak memberi tahu Anda saat pembaruan aturan terdeteksi.

Skenario	Apa yang dilakukan oleh Audit Manager	Apa yang perlu Anda lakukan
Aturan khusus diperbarui di instance Anda AWS Config.	Audit Manager terus melaporkan temuan untuk aturan tersebut menggunakan definisi aturan yang diperbarui.	Tidak ada tindakan yang diperlukan.
Aturan khusus dihapus di instance Anda AWS Config.	Audit Manager berhenti melaporkan temuan untuk aturan yang dihapus.	Tidak ada tindakan yang diperlukan. Jika mau, Anda dapat mengedit kontrol kustom yang menggunakan aturan yang dihapus sebagai pemetaan sumber data. Anda kemudian dapat menghapus aturan yang

Skenario	Apa yang dilakukan oleh Audit Manager	Apa yang perlu Anda lakukan
		dihapus untuk membersihkan pengaturan sumber data kontrol Anda. Jika tidak, nama aturan yang dihapus tetap sebagai pemetaan sumber data yang tidak digunakan.

Untuk pembaruan aturan di luar AWS lingkungan

Di AWS lingkungan penerima, Audit Manager tidak mendeteksi pembaruan aturan. Ini karena pengirim dan penerima masing-masing bekerja di AWS lingkungan yang terpisah. Tabel berikut memberikan tindakan yang disarankan untuk skenario ini.

Peran Anda	Skenario	Tindakan yang disarankan
Sender	- Anda berbagi kerangka kerja yang menggunakan aturan khusus sebagai pemetaan sumber data. - Setelah Anda membagikan kerangka kerja, Anda memperbarui atau menghapus salah satu aturan tersebut di AWS Config.	Hubungi penerima untuk memberi tahu mereka tentang pembaruan. Dengan begitu, mereka dapat membuat pembaruan yang sama dan tetap sinkron dengan definisi aturan terbaru.
Penerima	- Anda menerima kerangka kerja bersama yang menggunakan aturan khusus sebagai pemetaan sumber data. - Setelah Anda membuat ulang aturan khusus di instance Anda AWS Config, pengirim memperbarui atau menghapus salah satu aturan tersebut.	Buat pembaruan aturan yang sesuai di instance Anda sendiri AWS Config.

Memecahkan masalah pemberitahuan

Anda dapat menggunakan informasi di halaman ini untuk menyelesaikan masalah pemberitahuan umum di Audit Manager.

Topik

- [Saya menentukan topik Amazon SNS di Audit Manager, tetapi saya tidak menerima pemberitahuan apa pun](#)
- [Saya menentukan topik FIFO, tetapi saya tidak menerima notifikasi sesuai urutan yang diharapkan](#)

Saya menentukan topik Amazon SNS di Audit Manager, tetapi saya tidak menerima pemberitahuan apa pun

Jika topik Amazon SNS digunakan AWS KMS untuk enkripsi sisi server (SSE), Anda mungkin kehilangan izin yang diperlukan untuk kebijakan kunci Anda AWS KMS . Anda mungkin juga gagal menerima pemberitahuan jika Anda tidak berlangganan titik akhir untuk topik Anda.

Jika Anda tidak menerima notifikasi, pastikan Anda melakukan hal berikut:

- Anda melampirkan kebijakan izin yang diperlukan ke kunci KMS Anda. Untuk contoh kebijakan yang dapat Anda gunakan, lihat [Contoh 2 \(Izin untuk kunci KMS yang dilampirkan ke topik SNS\)](#).
- Anda berlangganan titik akhir ke topik yang dikirimkan notifikasi. Ketika Anda berlangganan titik akhir email ke topik, Anda menerima email yang meminta Anda untuk mengonfirmasi langganan Anda. Anda harus mengonfirmasi langganan Anda untuk mulai menerima pemberitahuan email. Untuk informasi selengkapnya, lihat Mem [ulai](#) di Panduan Pengembang Amazon SNS.

Saya menentukan topik FIFO, tetapi saya tidak menerima notifikasi sesuai urutan yang diharapkan

Audit Manager mendukung pengiriman pemberitahuan ke topik SNS FIFO. Namun, urutan Audit Manager mengirimkan notifikasi ke topik FIFO Anda tidak dijamin.

Memecahkan masalah izin dan akses

Anda dapat menggunakan informasi di halaman ini untuk menyelesaikan masalah izin umum di Audit Manager.

Topik

- [Saya mengikuti prosedur penyiapan Audit Manager, tetapi saya tidak memiliki cukup hak IAM](#)
- [Saya menentukan seseorang sebagai pemilik audit, tetapi mereka masih belum memiliki akses penuh ke penilaian. Mengapa ini?](#)
- [Saya tidak dapat melakukan tindakan di Manajer Audit](#)
- [Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses sumber daya Manajer Audit saya](#)
- [Saya melihat kesalahan Akses Ditolak, meskipun memiliki izin Audit Manager yang diperlukan](#)
- [Sumber daya tambahan](#)

Saya mengikuti prosedur penyiapan Audit Manager, tetapi saya tidak memiliki cukup hak IAM

Pengguna, peran, atau grup yang Anda gunakan untuk mengakses Audit Manager harus memiliki izin yang diperlukan. Selain itu, kebijakan berbasis identitas Anda seharusnya tidak terlalu membatasi. Jika tidak, konsol tidak akan berfungsi sebagaimana dimaksud. Panduan ini memberikan contoh kebijakan yang dapat Anda gunakan untuk [izinkan izin minimum yang diperlukan untuk mengaktifkan Audit Manager](#). Tergantung pada kasus penggunaan Anda, Anda mungkin memerlukan izin yang lebih luas dan tidak terlalu membatasi. Misalnya, sebaiknya pemilik audit memiliki akses [administrator](#). Hal ini agar mereka dapat mengubah pengaturan Audit Manager dan mengelola sumber daya seperti penilaian, kerangka kerja, kontrol, dan laporan penilaian. Pengguna lain, seperti delegasi, mungkin hanya memerlukan akses [manajemen](#) atau akses [baca-saja](#).

Pastikan Anda menambahkan izin yang sesuai untuk pengguna, peran, atau grup Anda. Untuk pemilik audit, kebijakan yang disarankan adalah [AWSAuditManagerAdministratorAccess](#). Untuk delegasi, Anda dapat menggunakan [kebijakan contoh akses manajemen](#) yang disediakan di [halaman contoh kebijakan](#) IAM. Anda dapat menggunakan contoh kebijakan ini sebagai titik awal, dan membuat perubahan yang diperlukan agar sesuai dengan kebutuhan Anda.

Kami menyarankan Anda meluangkan waktu untuk menyesuaikan izin Anda untuk memenuhi persyaratan spesifik Anda. Jika Anda memerlukan bantuan dengan izin IAM, hubungi administrator atau [AWS Dukungan](#) Anda.

Saya menentukan seseorang sebagai pemilik audit, tetapi mereka masih belum memiliki akses penuh ke penilaian. Mengapa ini?

Menentukan seseorang sebagai pemilik audit saja tidak memberi mereka akses penuh ke penilaian. Pemilik audit juga harus memiliki izin IAM yang diperlukan untuk mengakses dan mengelola sumber daya Audit Manager. Dengan kata lain, selain [menentukan pengguna sebagai pemilik audit](#), Anda juga harus melampirkan kebijakan IAM yang [diperlukan](#) untuk pengguna tersebut. Gagasan di balik ini adalah bahwa, dengan mengharuskan keduanya, Manajer Audit memastikan bahwa Anda memiliki kontrol penuh atas semua spesifikasi setiap penilaian.

Note

Untuk pemilik audit, kami sarankan Anda menggunakan [AWSAuditManagerAdministratorAccess](#) kebijakan tersebut. Untuk informasi selengkapnya, lihat [Kebijakan yang disarankan untuk persona pengguna di AWS Audit Manager](#).

Saya tidak dapat melakukan tindakan di Manajer Audit

Jika Anda tidak memiliki izin yang diperlukan untuk menggunakan operasi API AWS Audit Manager konsol atau Audit Manager, kemungkinan Anda akan mengalami `AccessDeniedException` kesalahan.

Untuk mengatasi masalah ini, Anda harus menghubungi administrator Anda untuk mendapatkan bantuan. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses sumber daya Manajer Audit saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah Audit Manager mendukung fitur-fitur ini, lihat [Bagaimana AWS Audit Manager bekerja dengan IAM](#).

- Untuk mempelajari cara menyediakan akses ke sumber daya di seluruh sumber daya Akun AWS yang Anda miliki, lihat [Menyediakan akses ke pengguna IAM lainnya Akun AWS yang Anda miliki](#) di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat [Menyediakan Akun AWS akan akses milik pihak ketiga](#) di Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat [Menyediakan akses ke pengguna terautentikasi eksternal \(federasi identitas\)](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya [lintas akun di IAM di Panduan Pengguna IAM](#).

Saya melihat kesalahan Akses Ditolak, meskipun memiliki izin Audit Manager yang diperlukan

Jika akun Anda adalah bagian dari organisasi, kemungkinan Access Denied kesalahan tersebut disebabkan oleh kebijakan kontrol [layanan \(SCP\)](#). SCP adalah kebijakan yang digunakan untuk mengelola izin untuk organisasi. Ketika SCP ada, SCP dapat menolak izin tertentu ke semua akun anggota, termasuk akun administrator yang didelegasikan yang Anda gunakan di Audit Manager.

Misalnya, jika organisasi Anda memiliki SCP yang menolak izin untuk API Katalog AWS Kontrol, Anda tidak dapat melihat sumber daya yang disediakan oleh Katalog Kontrol. Ini benar bahkan jika Anda memiliki izin yang diperlukan untuk Manajer Audit, seperti [AWSAuditManagerAdministratorAccess](#) kebijakan. SCP mengesampingkan izin kebijakan terkelola dengan secara eksplisit menolak akses ke API Katalog Kontrol.

Berikut adalah contoh SCP semacam itu. Dengan SCP ini, akun administrator yang didelegasikan ditolak akses ke kontrol umum, tujuan kontrol, dan domain kontrol yang diperlukan untuk menggunakan fitur kontrol umum di Audit Manager.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "controlcatalog:ListCommonControls",
```

```
        "controlcatalog:ListObjectives",
        "controlcatalog:ListDomains"
    ],
    "Resource": "*"
}
]
```

Untuk mengatasi masalah ini, kami sarankan Anda mengambil langkah-langkah berikut:

1. Konfirmasikan apakah SCP dilampirkan ke organisasi Anda. Untuk petunjuk, lihat [Mendapatkan informasi tentang kebijakan organisasi Anda](#) di Panduan Pengguna Organisasi AWS.
2. Identifikasi apakah SCP menyebabkan Access Denied kesalahan.
3. Perbarui SCP untuk memastikan bahwa akun administrator yang didelegasikan memiliki akses yang diperlukan untuk Manajer Audit. Untuk petunjuk, lihat [Memperbarui SCP](#) di Panduan Pengguna Organisasi AWS.

Sumber daya tambahan

Halaman berikut berisi panduan pemecahan masalah untuk masalah lain yang dapat disebabkan oleh hilangnya izin:

- [Saya tidak dapat melihat kontrol atau kumpulan kontrol apa pun dalam penilaian saya](#)
- [Opsi aturan khusus tidak tersedia saat saya mengonfigurasi sumber data kontrol](#)
- [Saya mendapatkan akses ditolak kesalahan saat saya mencoba membuat laporan](#)
- [Saya mendapatkan akses ditolak kesalahan saat saya mencoba membuat laporan penilaian menggunakan akun administrator yang didelegasikan](#)
- [Saya tidak dapat mengaktifkan pencari bukti](#)
- [Saya tidak dapat menonaktifkan pencari bukti](#)
- [Kueri pencarian saya gagal](#)
- [Saya menentukan topik Amazon SNS di Audit Manager, tetapi saya tidak menerima pemberitahuan apa pun](#)

Sumber daya penandaan AWS Audit Manager

Tag adalah label metadata yang Anda tetapkan atau yang ditetapkan ke sumber AWS daya. AWS Setiap tanda terdiri dari kunci dan nilai. Untuk tanda yang Anda tetapkan, Anda menentukan kunci dan nilai. Misalnya, Anda dapat menentukan kunci sebagai stage dan nilai untuk satu sumber daya sebagai test.

Tanda membantu Anda melakukan hal berikut:

- Temukan sumber daya Audit Manager Anda dengan mudah. Anda dapat menggunakan tag sebagai kriteria pencarian saat menjelajahi pustaka kerangka kerja dan pustaka kontrol.
- Kaitkan sumber daya Anda dengan jenis kepatuhan. Anda dapat menandai beberapa sumber daya dengan tag khusus kepatuhan untuk mengaitkan sumber daya tersebut dengan kerangka kerja tertentu.
- Identifikasi dan atur AWS sumber daya Anda. Banyak penandaan Layanan AWS dukungan, sehingga Anda dapat menetapkan tag yang sama ke sumber daya dari layanan yang berbeda untuk menunjukkan bahwa sumber daya terkait.
- Lacak AWS biaya Anda. Anda mengaktifkan tag ini di AWS Manajemen Penagihan dan Biaya dasbor. AWS menggunakan tag untuk mengkategorikan biaya Anda dan mengirimkan laporan alokasi biaya bulanan kepada Anda. Untuk informasi selengkapnya, lihat [Menggunakan tag alokasi biaya](#) di Panduan AWS Manajemen Penagihan dan Biaya Pengguna.

Bagian berikut memberikan informasi lebih lanjut tentang tag untuk AWS Audit Manager.

Daftar Isi

- [Sumber daya yang didukung di Audit Manager](#)
- [Batasan tag](#)
- [Sumber daya tambahan](#)

Sumber daya yang didukung di Audit Manager

Sumber daya Audit Manager berikut mendukung penandaan:

- Penilaian

- Kontrol
- Kerangka Kerja

Batasan tag

Pembatasan dasar berikut berlaku untuk tag pada sumber daya Audit Manager:

- Jumlah maksimum tag yang dapat Anda tetapkan ke sumber daya — 50
- Panjang kunci maksimum - 128 karakter Unicode
- Panjang nilai maksimum - 256 karakter Unicode
- Karakter yang valid untuk kunci dan nilai - a-z, A-Z, 0-9, spasi, dan karakter berikut: _./= + - dan @
- Kunci dan nilai bersifat peka huruf besar-kecil
- Jangan gunakan `aws :` sebagai awalan untuk kunci; itu dicadangkan untuk AWS digunakan

Sumber daya tambahan

Anda dapat menetapkan tag sebagai properti saat membuat penilaian, kerangka kerja, atau kontrol. Anda dapat menambahkan, mengedit, dan menghapus tag melalui konsol Audit Manager, AWS Command Line Interface (AWS CLI), dan Audit Manager API. Untuk informasi lebih lanjut, lihat tautan berikut.

- Untuk penilaian penandaan:
 - [Membuat penilaian di AWS Audit Manager](#) dan [Mengedit penilaian di AWS Audit Manager](#) di bagian Penilaian dari panduan ini
 - [Tab tag](#) di halaman Tinjau penilaian panduan ini
 - [CreateAssessment](#) dan [UpdateAssessment](#) di Referensi AWS Audit Manager API
 - [TagResource](#) dan [UntagResource](#) di Referensi AWS Audit Manager API
- Untuk kerangka kerja penandaan:
 - [Membuat kerangka kerja khusus di AWS Audit Manager](#) dan [Mengedit kerangka kerja khusus di AWS Audit Manager](#) di bagian pustaka Framework dari panduan ini
 - [Tags tab](#) Pada halaman Lihat rincian kerangka kerja dari panduan ini
 - [CreateAssessmentFramework](#) dan [UpdateAssessmentFramework](#) di Referensi AWS Audit Manager API

- [TagResource](#) dan [UntagResource](#) di Referensi AWS Audit Manager API
- Untuk kontrol penandaan:
 - [Membuat kontrol khusus di AWS Audit Manager](#) dan [Mengedit kontrol khusus di AWS Audit Manager](#) di bagian Control library dari panduan ini
 - [Tags](#) Bagian pada halaman Meninjau kontrol kustom dari panduan ini
 - [Tags](#) Bagian pada halaman Meninjau kontrol standar panduan ini
 - [CreateControl](#) dan [UpdateControl](#) di Referensi AWS Audit Manager API
 - [TagResource](#) dan [UntagResource](#) di Referensi AWS Audit Manager API

Memahami kuota dan batasan untuk AWS Audit Manager

Anda Akun AWS memiliki kuota default, sebelumnya disebut sebagai batas, untuk masing-masing Layanan AWS Kecuali dinyatakan lain, setiap kuota adalah Region-specific. Anda dapat meminta kenaikan untuk beberapa kuota, dan kuota lainnya tidak dapat ditingkatkan.

Sebagian besar kuota Audit Manager, tetapi tidak semua, tercantum di bawah AWS Audit Manager namespace di konsol Service Quotas. Untuk mempelajari cara meminta peningkatan kuota, lihat [Mengelola kuota Audit Manager Anda](#).

Daftar Isi

- [Kuota Audit Manager default](#)
- [Mengelola kuota Audit Manager Anda](#)
- [Sumber daya tambahan](#)

Kuota Audit Manager default

AWS Audit Manager Kuota berikut adalah Akun AWS per Wilayah.

Sumber daya	Kuota
Penilaian	Jumlah penilaian aktif per akun: 100
Kontrol	Jumlah kontrol khusus per akun: 500
Bukti	Ukuran maksimum satu file bukti manual: 100 MB
	Jumlah unggahan bukti manual harian per kontrol: 100
 Tip Jika Anda perlu mengunggah sejumlah besar bukti manual ke satu kontrol, kami sarankan Anda mengunggah bukti Anda dalam batch selama beberapa hari.	
Kerangka	Jumlah kerangka kerja khusus per akun: 100

Sumber daya	Kuota
	 Note Kuota kerangka berlaku untuk semua kerangka kerja kustom bersama di pustaka kerangka kerja Anda, terlepas dari siapa yang membuat kerangka kerja.
Penerima kerangka kustom bersama	Jumlah akun penerima aktif: 100
Akses API	Jumlah transaksi per detik (TPS) di semua API: 20 TPS

Mengelola kuota Audit Manager Anda

AWS Audit Manager terintegrasi dengan Service Quotas, sebuah Layanan AWS yang memungkinkan Anda untuk melihat dan mengelola kuota Anda dari lokasi pusat. Service Quotas memudahkan untuk mencari nilai kuota Audit Manager Anda.

Untuk melihat kuota layanan Audit Manager menggunakan konsol

1. Buka konsol Service Quotas di <https://console.aws.amazon.com/servicequotas/>.
2. Di panel navigasi, pilih Layanan AWS.
3. Dari Layanan AWS daftar, cari dan pilih AWS Audit Manager.
4. Dalam daftar Kuota layanan, Anda dapat melihat nama kuota layanan, nilai kuota yang diterapkan (jika tersedia), nilai kuota AWS default, dan apakah kuota dapat disesuaikan.
5. Untuk melihat informasi tambahan tentang service quotas, seperti deskripsi, pilih nama kuota.
6. (Opsional) Untuk meminta peningkatan kuota, pilih kuota yang ingin Anda tingkatkan, kemudian pilih Meminta peningkatan kuota, masukkan atau pilih informasi yang diperlukan, dan pilih Minta.

Sumber daya tambahan

Untuk informasi selengkapnya tentang cara mengelola kuota, lihat [Meminta peningkatan kuota di Panduan Pengguna Service Quotas](#).

Untuk informasi selengkapnya tentang Service Quotas, lihat [Apa itu Service Quotas?](#) dalam Panduan Pengguna Service Quotas.

Contoh kode untuk Audit Manager menggunakan AWS SDKs

Contoh kode berikut menunjukkan cara menggunakan Audit Manager dengan AWS software development kit (SDK).

Skenario adalah contoh kode yang menunjukkan kepada Anda bagaimana menyelesaikan tugas tertentu dengan memanggil beberapa fungsi dalam layanan atau dikombinasikan dengan yang lain Layanan AWS.

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Penggunaan AWS Audit Manager dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Contoh kode

- [Skenario untuk Audit Manager menggunakan AWS SDKs](#)
 - [Membuat framework kustom Audit Manager dari paket AWS Config kesesuaian menggunakan SDK AWS](#)
 - [Membuat kerangka kerja khusus Audit Manager yang berisi kontrol CSPM Security Hub menggunakan SDK AWS](#)
 - [Membuat laporan penilaian Audit Manager yang berisi bukti satu hari menggunakan AWS SDK](#)

Skenario untuk Audit Manager menggunakan AWS SDKs

Contoh kode berikut menunjukkan cara menerapkan skenario umum di Audit Manager dengan AWS SDKs. Skenario ini menunjukkan kepada Anda cara menyelesaikan tugas tertentu dengan memanggil beberapa fungsi dalam Audit Manager atau digabungkan dengan yang lain Layanan AWS. Setiap skenario menyertakan tautan ke kode sumber lengkap, di mana Anda dapat menemukan instruksi tentang cara mengatur dan menjalankan kode.

Skenario menargetkan tingkat pengalaman menengah untuk membantu Anda memahami tindakan layanan dalam konteks.

Contoh

- [Membuat framework kustom Audit Manager dari paket AWS Config kesesuaian menggunakan SDK AWS](#)

- [Membuat kerangka kerja khusus Audit Manager yang berisi kontrol CSPM Security Hub menggunakan SDK AWS](#)
- [Membuat laporan penilaian Audit Manager yang berisi bukti satu hari menggunakan AWS SDK](#)

Membuat framework kustom Audit Manager dari paket AWS Config kesesuaian menggunakan SDK AWS

Contoh kode berikut ini menunjukkan cara untuk melakukan:

- Dapatkan daftar paket AWS Config kesesuaian.
- Buat kontrol kustom Audit Manager untuk setiap aturan terkelola dalam paket kesesuaian.
- Buat kerangka kerja khusus Audit Manager yang berisi kontrol.

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
import logging
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)

class ConformancePack:
    def __init__(self, config_client, auditmanager_client):
        self.config_client = config_client
        self.auditmanager_client = auditmanager_client

    def get_conformance_pack(self):
        """
        Return a selected conformance pack from the list of conformance packs.
```

```

:return: selected conformance pack
"""
try:
    conformance_packs = self.config_client.describe_conformance_packs()
    print(
        "Number of conformance packs fetched: ",
        len(conformance_packs.get("ConformancePackDetails")),
    )
    print("Fetched the following conformance packs: ")
    all_cpack_names = {
        cp["ConformancePackName"]
        for cp in conformance_packs.get("ConformancePackDetails")
    }
    for pack in all_cpack_names:
        print(f"\t{pack}")
    cpack_name = input(
        "Provide ConformancePackName that you want to create a custom "
        "framework for: "
    )
    if cpack_name not in all_cpack_names:
        print(f"{cpack_name} is not in the list of conformance packs!")
        print(
            "Provide a conformance pack name from the available list of "
            "conformance packs."
        )
        raise Exception("Invalid conformance pack")
    print("-" * 88)
except ClientError:
    logger.exception("Couldn't select conformance pack.")
    raise
else:
    return cpack_name

def create_custom_controls(self, cpack_name):
    """
    Create custom controls for all managed AWS Config rules in a conformance
    pack.

    :param cpack_name: The name of the conformance pack to create controls
    for.

    :return: The list of custom control IDs.
    """
    try:

```



```

        rules_in_pack =
self.config_client.describe_conformance_pack_compliance(
    ConformancePackName=cpack_name
)
print(
    "Number of rules in the conformance pack: ",
    len(rules_in_pack.get("ConformancePackRuleComplianceList")),
)
for rule in rules_in_pack.get("ConformancePackRuleComplianceList"):
    print(f"\t{rule.get('ConfigRuleName')}")
print("-" * 88)
print(
    "Creating a custom control for each rule and a custom framework "
    "consisting of these rules in Audit Manager."
)
am_controls = []
for rule in rules_in_pack.get("ConformancePackRuleComplianceList"):
    config_rule = self.config_client.describe_config_rules(
        ConfigRuleNames=[rule.get("ConfigRuleName")]
    )
    source_id = (
        config_rule.get("ConfigRules")[0]
        .get("Source", {})
        .get("SourceIdentifier")
    )
    custom_control = self.auditmanager_client.create_control(
        name="Config-" + rule.get("ConfigRuleName"),
        controlMappingSources=[
            {
                "sourceName": "ConfigRule",
                "sourceSetUpOption": "System_Controls_Mapping",
                "sourceType": "AWS_Config",
                "sourceKeyword": {
                    "keywordInputType": "SELECT_FROM_LIST",
                    "keywordValue": source_id,
                },
            },
        ],
    ).get("control", {})
    am_controls.append({"id": custom_control.get("id")})
print("Successfully created a control for each config rule.")
print("-" * 88)
except ClientError:
    logger.exception("Failed to create custom controls.")

```

```

        raise
    else:
        return am_controls

def create_custom_framework(self, cpack_name, am_control_ids):
    """
    Create a custom Audit Manager framework from a selected AWS Config
    conformance
    pack.

    :param cpack_name: The name of the conformance pack to create a framework
    from.
    :param am_control_ids: The IDs of the custom controls created from the
    conformance pack.
    """
    try:
        print("Creating custom framework...")
        custom_framework =
self.auditmanager_client.create_assessment_framework(
            name="Config-Conformance-pack-" + cpack_name,
            controlSets=[{"name": cpack_name, "controls": am_control_ids}],
        )
        print(
            f"Successfully created the custom framework: ",
            f"{custom_framework.get('framework').get('name')}: ",
            f"{custom_framework.get('framework').get('id')}",
        )
        print("-" * 88)
    except ClientError:
        logger.exception("Failed to create custom framework.")
        raise

def run_demo():
    print("-" * 88)
    print("Welcome to the AWS Audit Manager custom framework demo!")
    print("-" * 88)
    print(
        "You can use this sample to select a conformance pack from AWS Config and
"
        "use AWS Audit Manager to create a custom control for all the managed "
        "rules under the conformance pack. A custom framework is also created "
        "with these controls."
    )

```

```
print("-" * 88)
conf_pack = ConformancePack(boto3.client("config"),
boto3.client("auditmanager"))
cpack_name = conf_pack.get_conformance_pack()
am_controls = conf_pack.create_custom_controls(cpack_name)
conf_pack.create_custom_framework(cpack_name, am_controls)

if __name__ == "__main__":
    run_demo()
```

- Untuk detail API, lihat topik berikut ini adalah Referensi API SDK untuk Python (Boto3)AWS
 - [CreateAssessmentFramework](#)
 - [CreateControl](#)

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Penggunaan AWS Audit Manager dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Membuat kerangka kerja khusus Audit Manager yang berisi kontrol CSPM Security Hub menggunakan SDK AWS

Contoh kode berikut ini menunjukkan cara untuk melakukan:

- Dapatkan daftar semua kontrol standar yang memiliki Security Hub CSPM sebagai sumber datanya.
- Buat kerangka kerja khusus Audit Manager yang berisi kontrol.

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```

import logging
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)

class SecurityHub:
    def __init__(self, auditmanager_client):
        self.auditmanager_client = auditmanager_client

    def get_sechub_controls(self):
        """
        Gets the list of controls that use Security Hub as their data source.

        :return: The list of Security Hub controls.
        """
        print("-" * 88)
        next_token = None
        page = 1
        sechub_control_list = []
        while True:
            print("Page [" + str(page) + "]")
            if next_token is None:
                control_list = self.auditmanager_client.list_controls(
                    controlType="Standard", maxResults=100
                )
            else:
                control_list = self.auditmanager_client.list_controls(
                    controlType="Standard", nextToken=next_token, maxResults=100
                )
            print("Total controls found:",
len(control_list.get("controlMetadataList")))
            for control in control_list.get("controlMetadataList"):
                control_details = self.auditmanager_client.get_control(
                    controlId=control.get("id")
                ).get("control", {})
                if "AWS Security Hub" in control_details.get("controlSources"):
                    sechub_control_list.append({"id": control_details.get("id")})
            next_token = control_list.get("nextToken")
            if not next_token:
                break
            page += 1

```

```

        print("Number of Security Hub controls found: ",
              len(sechub_control_list))
        return sechub_control_list

    def create_custom_framework(self, am_controls):
        """
        Create a custom framework with a list of controls.

        :param am_controls: The list of controls to include in the framework.
        """
        try:
            print("Creating custom framework...")
            custom_framework =
self.auditmanager_client.create_assessment_framework(
                name="All Security Hub Controls Framework",
                controlSets=[{"name": "Security-Hub", "controls": am_controls}],
            )
            print(
                f"Successfully created the custom framework: "
                f"{custom_framework.get('framework').get('name')}: "
                f"{custom_framework.get('framework').get('id')}"
            )
            print("-" * 88)
        except ClientError:
            logger.exception("Failed to create custom framework.")
            raise

def run_demo():
    print("-" * 88)
    print("Welcome to the AWS Audit Manager Security Hub demo!")
    print("-" * 88)
    print(" This script creates a custom framework with all Security Hub
controls.")
    print("-" * 88)
    sechub = SecurityHub(boto3.client("auditmanager"))
    am_controls = sechub.get_sechub_controls()
    sechub.create_custom_framework(am_controls)

if __name__ == "__main__":
    run_demo()

```

- Untuk detail API, lihat topik berikut ini adalah Referensi API SDK untuk Python (Boto3)AWS
 - [CreateAssessmentFramework](#)
 - [GetControl](#)
 - [ListControls](#)

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Penggunaan AWS Audit Manager dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Membuat laporan penilaian Audit Manager yang berisi bukti satu hari menggunakan AWS SDK

Contoh kode berikut menunjukkan cara membuat laporan penilaian Audit Manager yang berisi bukti satu hari.

Python

SDK untuk Python (Boto3)

Note

Ada lebih banyak tentang GitHub. Temukan contoh lengkapnya dan pelajari cara mengatur dan menjalankannya di [Repositori Contoh Kode AWS](#).

```
import dateutil.parser
import logging
import time
import urllib.request
import uuid
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)

class AuditReport:
```

```

def __init__(self, auditmanager_client):
    self.auditmanager_client = auditmanager_client

def get_input(self):
    print("-" * 40)
    try:
        assessment_id = input("Provide assessment id [uuid]: ").lower()
        try:
            assessment_uuid = uuid.UUID(assessment_id)
        except ValueError:
            logger.error("Assessment Id is not a valid UUID: %s",
assessment_id)
            raise
        evidence_folder = input("Provide evidence date [yyyy-mm-dd]: ")
        try:
            evidence_date = dateutil.parser.parse(evidence_folder).date()
        except ValueError:
            logger.error("Invalid date : %s", evidence_folder)
            raise
        try:
            self.auditmanager_client.get_assessment(
                assessmentId=str(assessment_uuid)
            )
        except ClientError:
            logger.exception("Couldn't get assessment %s.", assessment_uuid)
            raise
    except (ValueError, ClientError):
        return None, None
    else:
        return assessment_uuid, evidence_date

def clear_staging(self, assessment_uuid, evidence_date):
    """
    Find all the evidence in the report and clear it.
    """
    next_token = None
    page = 1
    interested_folder_id_list = []
    while True:
        print(f"Page [{page}]")
        if next_token is None:
            folder_list = (
                self.auditmanager_client.get_evidence_folders_by_assessment(
                    assessmentId=str(assessment_uuid), maxResults=1000

```

```

        )
    )
else:
    folder_list = (
        self.auditmanager_client.get_evidence_folders_by_assessment(
            assessmentId=str(assessment_uuid),
            nextToken=next_token,
            maxResults=1000,
        )
    )
    folders = folder_list.get("evidenceFolders")
    print(f"Got {len(folders)} folders.")
    for folder in folders:
        folder_id = folder.get("id")
        if folder.get("name") == str(evidence_date):
            interested_folder_id_list.append(folder_id)
        if folder.get("assessmentReportSelectionCount") == folder.get(
            "totalEvidence"
        ):
            print(
                f"Removing folder from report selection :
{folder.get('name')} "
                f"{folder_id} {folder.get('controlId')}"
            )

    self.auditmanager_client.disassociate_assessment_report_evidence_folder(
        assessmentId=str(assessment_uuid),
        evidenceFolderId=folder_id
    )
    elif folder.get("assessmentReportSelectionCount") > 0:
        # Get all evidence in the folder and
        # add selected evidence in the selected_evidence_list.
        evidence_list = (
            self.auditmanager_client.get_evidence_by_evidence_folder(
                assessmentId=str(assessment_uuid),
                controlSetId=folder_id,
                evidenceFolderId=folder_id,
                maxResults=1000,
            )
        )
        selected_evidence_list = []
        for evidence in evidence_list.get("evidence"):
            if evidence.get("assessmentReportSelection") == "Yes":
                selected_evidence_list.append(evidence.get("id"))

```



```

        print(
            f"Removing evidence report selection :
{folder.get('name')} "
            f"{len(selected_evidence_list)}"
        )

self.auditmanager_client.batch_disassociate_assessment_report_evidence(
    assessmentId=str(assessment_uuid),
    evidenceFolderId=folder_id,
    evidenceIds=selected_evidence_list,
)
next_token = folder_list.get("nextToken")
if not next_token:
    break
page += 1
return interested_folder_id_list

def add_folder_to_staging(self, assessment_uuid, folder_id_list):
    print(f"Adding folders to report : {folder_id_list}")
    for folder in folder_id_list:
        self.auditmanager_client.associate_assessment_report_evidence_folder(
            assessmentId=str(assessment_uuid), evidenceFolderId=folder
        )

def get_report(self, assessment_uuid):
    report = self.auditmanager_client.create_assessment_report(
        name="ReportViaScript",
        description="testing",
        assessmentId=str(assessment_uuid),
    )
    if self._is_report_generated(report.get("assessmentReport").get("id")):
        report_url = self.auditmanager_client.get_assessment_report_url(
            assessmentReportId=report.get("assessmentReport").get("id"),
            assessmentId=str(assessment_uuid),
        )
        print(report_url.get("preSignedUrl"))
        urllib.request.urlretrieve(
            report_url.get("preSignedUrl").get("link"),
            report_url.get("preSignedUrl").get("hyperlinkName"),
        )
        print(
            f"Report saved as
{report_url.get('preSignedUrl').get('hyperlinkName')}. "
        )

```

```

        else:
            print("Report generation did not finish in 15 minutes.")
            print(
                "Failed to download report. Go to the console and manually
download "
                "the report."
            )

    def _is_report_generated(self, assessment_report_id):
        max_wait_time = 0
        while max_wait_time < 900:
            print(f"Checking status of the report {assessment_report_id}")
            report_list =
self.auditmanager_client.list_assessment_reports(maxResults=1)
            if (
                report_list.get("assessmentReports")[0].get("id")
                == assessment_report_id
                and report_list.get("assessmentReports")[0].get("status") ==
"COMPLETE"
            ):
                return True
            print("Sleeping for 5 seconds...")
            time.sleep(5)
            max_wait_time += 5

def run_demo():
    print("-" * 88)
    print("Welcome to the AWS Audit Manager samples demo!")
    print("-" * 88)
    print(
        "This script creates an assessment report for an assessment with all the
"
        "evidence collected on the provided date."
    )
    print("-" * 88)

    report = AuditReport(boto3.client("auditmanager"))
    assessment_uuid, evidence_date = report.get_input()
    if assessment_uuid is not None and evidence_date is not None:
        folder_id_list = report.clear_staging(assessment_uuid, evidence_date)
        report.add_folder_to_staging(assessment_uuid, folder_id_list)
        report.get_report(assessment_uuid)

```

```
if __name__ == "__main__":  
    run_demo()
```

- Untuk detail API, lihat topik berikut ini adalah Referensi API SDK untuk Python (Boto3)AWS
 - [AssociateAssessmentReportEvidenceFolder](#)
 - [BatchDisassociateAssessmentReportEvidence](#)
 - [CreateAssessmentReport](#)
 - [DisassociateAssessmentReportEvidenceFolder](#)
 - [GetAssessment](#)
 - [GetAssessmentReportUrl](#)
 - [GetEvidenceByEvidenceFolder](#)
 - [GetEvidenceFoldersByAssessment](#)
 - [ListAssessmentReports](#)

Untuk daftar lengkap panduan pengembang AWS SDK dan contoh kode, lihat [Penggunaan AWS Audit Manager dengan AWS SDK](#). Topik ini juga mencakup informasi tentang memulai dan detail tentang versi SDK sebelumnya.

Memahami keamanan dan perlindungan data di AWS Audit Manager

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama AWS antara Anda. [Model tanggung jawab bersama](#) menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- **Keamanan cloud** — AWS bertanggung jawab untuk melindungi infrastruktur yang berjalan Layanan AWS di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Third-party auditor secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program Kep [AWS atuhan Program Kep](#) . Untuk mempelajari tentang program kepatuhan yang berlaku untuk AWS Audit Manager, lihat [AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan](#) .
- **Keamanan di cloud** — Tanggung jawab Anda ditentukan oleh apa Layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan AWS Audit Manager. Topik berikut menunjukkan cara mengonfigurasi Audit Manager untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan Layanan AWS yang lain yang membantu Anda memantau dan mengamankan sumber daya Manajer Audit Anda.

Topik

- [Perlindungan data di AWS Audit Manager](#)
- [Identitas dan manajemen akses untuk AWS Audit Manager](#)
- [Validasi kepatuhan untuk AWS Audit Manager](#)
- [Memahami ketahanan dalam AWS Audit Manager](#)
- [Keamanan infrastruktur di AWS Audit Manager](#)
- [AWS Audit Manager dan antarmuka titik akhir VPC \(AWS PrivateLink\)](#)
- [Pencatatan dan pemantauan di AWS Audit Manager](#)

- [Memahami konfigurasi dan analisis kerentanan di AWS Audit Manager](#)

Perlindungan data di AWS Audit Manager

[Model tanggung jawab bersama](#) AWS berlaku untuk perlindungan data di AWS Audit Manager. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat FAQ Privasi [Data Ket](#) . Untuk informasi tentang perlindungan data di Eropa, lihat [Pusat Peraturan Umum Perlindungan Data \(GDPR\)](#).

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensial dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang menggunakan CloudTrail jalur untuk menangkap AWS aktivitas, lihat [Bekerja dengan CloudTrail jejak](#) di Panduan AWS CloudTrail Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di [Standar Pemrosesan Informasi Federal \(FIPS\) 140-3](#).

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Audit Manager atau lainnya Layanan AWS

menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Selain rekomendasi di atas, kami merekomendasikan secara khusus agar pelanggan Audit Manager tidak menyertakan informasi identifikasi sensitif dalam bidang bentuk bebas saat membuat penilaian, kontrol khusus, kerangka kerja khusus, dan komentar delegasi.

Penghapusan data Audit Manager

Ada beberapa cara agar data Audit Manager dapat dihapus.

Penghapusan data saat menonaktifkan Audit Manager

Saat [menonaktifkan Audit Manager](#), Anda dapat memutuskan apakah Anda ingin menghapus semua data Manajer Audit Anda. Jika Anda memilih untuk menghapus data, data akan dihapus dalam waktu 7 hari setelah menonaktifkan Audit Manager. Setelah data dihapus, Anda tidak dapat memulihkannya.

Penghapusan data otomatis

Beberapa data Audit Manager dihapus secara otomatis setelah jangka waktu tertentu. Audit Manager menyimpan data pelanggan sebagai berikut.

Jenis data	Periode retensi data	Catatan
Bukti	Data disimpan selama 2 tahun sejak saat pembuatan	Termasuk bukti otomatis dan bukti manual
Customer-created sumber daya	Data disimpan tanpa batas	Termasuk penilaian, laporan penilaian, kontrol khusus, dan kerangka kerja khusus

Penghapusan data manual

Anda dapat menghapus sumber daya Manajer Audit individual kapan saja. Untuk petunjuk, lihat yang berikut ini:

- [Menghapus penilaian di AWS Audit Manager](#)
 - Lihat juga: [DeleteAssessment](#) di Refer AWS Audit Manager ensi API
- [Menghapus kerangka kerja khusus di AWS Audit Manager](#)
 - Lihat juga: [DeleteAssessmentFramework](#) di Refer AWS Audit Manager ensi API
- [Menghapus permintaan berbagi di AWS Audit Manager](#)
 - Lihat juga: [DeleteAssessmentFrameworkShare](#) di Refer AWS Audit Manager ensi API
- [Menghapus laporan penilaian](#)
 - Lihat juga: [DeleteAssessmentReport](#) di Refer AWS Audit Manager ensi API
- [Menghapus kontrol khusus di AWS Audit Manager](#)
 - Lihat juga: [DeleteControl](#) di Refer AWS Audit Manager ensi API

Untuk menghapus data sumber daya lain yang mungkin telah Anda buat saat menggunakan Audit Manager, lihat berikut ini:

- [Menghapus penyimpanan data peristiwa](#) di Panduan AWS CloudTrail Pengguna
- [Menghapus bucket](#) di Panduan Pengguna Amazon Simple Storage Service (Amazon S3)

Enkripsi saat diam

Untuk mengenkripsi data saat diam, Audit Manager menggunakan enkripsi sisi server dengan Kunci yang dikelola AWS semua penyimpanan data dan log.

Data Anda dienkripsi di bawah kunci yang dikelola pelanggan atau Kunci milik AWS, tergantung pada pengaturan yang Anda pilih. Jika Anda tidak memberikan kunci yang dikelola pelanggan, Audit Manager menggunakan kunci Kunci milik AWS untuk mengenkripsi konten Anda. Semua metadata layanan di DynamoDB dan Amazon S3 di Audit Manager dienkripsi menggunakan Kunci milik AWS

Audit Manager mengenkripsi data sebagai berikut:

- Metadata layanan yang disimpan di Amazon S3 dienkripsi di bawah Kunci milik AWS penggunaan SSE-KMS.
- Metadata layanan yang disimpan di DynamoDB dienkripsi sisi server menggunakan KMS dan an. Kunci milik AWS

- Konten Anda yang disimpan di DynamoDB dienkripsi sisi klien menggunakan kunci yang dikelola pelanggan atau. Kunci milik AWS Kunci KMS didasarkan pada pengaturan yang Anda pilih.
- Konten Anda yang disimpan di Amazon S3 di Audit Manager dienkripsi menggunakan SSE-KMS. Kunci KMS didasarkan pada pilihan Anda, dan bisa berupa kunci yang dikelola pelanggan atau kunci. Kunci milik AWS
- Laporan penilaian yang dipublikasikan ke bucket S3 Anda dienkripsi sebagai berikut:
 - Jika Anda memberikan kunci yang dikelola pelanggan, data Anda dienkripsi menggunakan SSE-KMS.
 - Jika Anda menggunakan Kunci milik AWS, data Anda dienkripsi menggunakan SSE-S3.

Enkripsi saat bergerak

Audit Manager menyediakan titik akhir yang aman dan pribadi untuk mengenkripsi data dalam transit. Titik akhir yang aman dan pribadi memungkinkan AWS untuk melindungi integritas permintaan API ke Audit Manager.

Inter-service transit

Secara default, semua komunikasi antar layanan dilindungi dengan menggunakan enkripsi Transport Layer Security (TLS).

Manajemen kunci

Audit Manager mendukung kedua kunci Kunci milik AWS dan kunci yang dikelola pelanggan untuk mengenkripsi semua sumber daya Audit Manager (penilaian, kontrol, kerangka kerja, bukti, dan laporan penilaian yang disimpan ke bucket S3 di akun Anda).

Sebaiknya gunakan kunci yang dikelola pelanggan. Dengan demikian, Anda dapat melihat dan mengelola kunci enkripsi yang melindungi data Anda, termasuk melihat log penggunaannya di AWS CloudTrail. Saat Anda memilih kunci yang dikelola pelanggan, Audit Manager membuat hibah pada kunci KMS sehingga dapat digunakan untuk mengenkripsi konten Anda.

Warning

Setelah menghapus atau menonaktifkan kunci KMS yang digunakan untuk mengenkripsi sumber daya Audit Manager, Anda tidak dapat lagi mendekripsi sumber daya yang dienkripsi di bawah kunci KMS tersebut, yang berarti data menjadi tidak dapat dipulihkan.

Menghapus kunci KMS di AWS Key Management Service (AWS KMS) bersifat merusak dan berpotensi berbahaya. Untuk informasi selengkapnya tentang menghapus kunci KMS, lihat [Mengh AWS KMS keys](#) apus di Panduan AWS Key Management Service Pengguna.

Anda dapat menentukan setelan enkripsi saat mengaktifkan Audit Manager menggunakan Konsol Manajemen AWS, Audit Manager API, atau AWS Command Line Interface (AWS CLI). Untuk petunjuk, lihat [Mengaktifkan AWS Audit Manager](#).

Anda dapat meninjau dan mengubah pengaturan enkripsi kapan saja. Untuk petunjuk, lihat [Mengkonfigurasi pengaturan enkripsi data Anda](#).

Untuk informasi selengkapnya tentang cara mengatur kunci yang dikelola pelanggan, lihat [Membuat kunci](#) di Panduan AWS Key Management Service Pengguna.

Identitas dan manajemen akses untuk AWS Audit Manager

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan di otorisasi (memiliki izin) untuk menggunakan sumber daya Audit Manager. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)
- [Mengelola akses menggunakan kebijakan](#)
- [Bagaimana AWS Audit Manager bekerja dengan IAM](#)
- [Identity-based Contoh kebijakan untuk AWS Audit Manager](#)
- [Cross-service pencegahan wakil yang bingung](#)
- [Resource-based Contoh kebijakan untuk AWS Audit Manager](#)
- [AWS kebijakan yang dikelola untuk AWS Audit Manager](#)
- [Pemecahan masalah AWS Audit Manager Identitas dan Akses](#)
- [Menggunakan peran terkait layanan untuk AWS Audit Manager](#)

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda berdasarkan peran Anda:

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat [Pemecahan masalah AWS Audit Manager Identitas dan Akses](#))
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat [Bagaimana AWS Audit Manager bekerja dengan IAM](#))
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat [Identity-based Contoh kebijakan untuk AWS Audit Manager](#))

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredentif identitas Anda. Anda harus diautentikasi sebagai Pengguna root akun AWS, pengguna IAM, atau dengan mengambil peran IAM.

Anda dapat masuk sebagai identitas federasi menggunakan kredenSIAL dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), otentikasi masuk tunggal, atau kredenSIAL. Google/Facebook Untuk informasi selengkapnya tentang cara masuk, lihat [Cara masuk ke Akun AWS Anda](#) dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS menyediakan SDK dan CLI untuk menandatangani permintaan kriptografis. Untuk informasi selengkapnya, lihat [AWS Signature Version 4 untuk permintaan API](#) dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat [Tugas yang memerlukan kredensial pengguna root](#) dalam Panduan Pengguna IAM.

Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS menggunakan kredenSIAL sementara.

Identitas federasi adalah pengguna dari direktori perusahaan Anda, penyedia identitas web, atau Directory Service yang mengakses Layanan AWS menggunakan kredensial dari sumber identitas. Identitas terfederasi mengambil peran yang memberikan kredensial sementara.

Untuk manajemen akses terpusat, kami menyarankan AWS IAM Identity Center. Untuk informasi selengkapnya, lihat [Apa itu Pusat Identitas IAM?](#) dalam Panduan Pengguna AWS IAM Identity Center.

Pengguna dan grup IAM

[Pengguna IAM](#) adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk informasi selengkapnya, lihat [Memerlukan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensial sementara](#) di Panduan Pengguna IAM.

[Grup IAM](#) menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat [Kasus penggunaan untuk pengguna IAM](#) dalam Panduan Pengguna IAM.

Peran IAM

[Peran IAM](#) adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan [beralih dari pengguna ke peran IAM \(konsol\)](#) atau dengan memanggil operasi AWS CLI AWS API. Untuk informasi selengkapnya, lihat [Metode untuk mengambil peran](#) dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna terfederasi, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon EC2. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat [Gambaran umum kebijakan JSON](#) dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukan operasinya.

Identity-based kebijakan

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan](#) dalam Panduan Pengguna IAM.

Identity-based kebijakan dapat berupa kebijakan sebaris (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan ke beberapa identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat [Pilih antara kebijakan terkelola dan kebijakan inline](#) dalam Panduan Pengguna IAM.

Resource-based kebijakan

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya.

Resource-based kebijakan adalah kebijakan sebaris yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat mengatur izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat [Batasan izin untuk entitas IAM](#) dalam Panduan Pengguna IAM.

- Kebijakan kontrol layanan (SCP) – Menentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat [Kebijakan kontrol layanan](#) dalam Panduan Pengguna AWS Organizations .
- Kebijakan kontrol sumber daya (RCP) – Menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat [Kebijakan kontrol sumber daya \(RCP\)](#) dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat [Kebijakan sesi](#) dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan ketika beberapa jenis kebijakan terlibat, lihat Logika evaluasi [kebijakan](#) di Panduan Pengguna IAM.

Bagaimana AWS Audit Manager bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Audit Manager, pelajari fitur IAM apa yang tersedia untuk digunakan dengan Audit Manager.

Fitur IAM yang dapat Anda gunakan AWS Audit Manager

Fitur IAM	Dukungan Manajer Audit
Identity-based kebijakan	Ya
Resource-based kebijakan	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Parsial
ACL	Tidak
ABAC (tanda dalam kebijakan)	Ya

Fitur IAM	Dukungan Manajer Audit
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya
Peran layanan	Tidak
Service-linked peran	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara AWS Audit Manager dan AWS layanan lain bekerja dengan sebagian besar fitur IAM, lihat [AWS layanan yang bekerja dengan IAM](#) di Panduan Pengguna IAM.

Identity-based kebijakan untuk AWS Audit Manager

Mendukung kebijakan berbasis identitas: Ya

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke identitas, seperti pengguna IAM, grup pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan](#) dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat [Referensi elemen kebijakan JSON IAM](#) dalam Panduan Pengguna IAM.

AWS Audit Manager membuat kebijakan terkelola yang dinam `AWSAuditManagerAdministratorAccess` di administrator Audit Manager. Kebijakan ini memberikan akses administrasi penuh di Audit Manager. Administrator dapat melampirkan kebijakan ini ke peran atau pengguna yang ada, atau membuat peran baru dengan kebijakan ini.

Kebijakan yang disarankan untuk persona pengguna di AWS Audit Manager

AWS Audit Manager memungkinkan Anda mempertahankan pemisahan tugas di antara pengguna yang berbeda dan untuk audit yang berbeda dengan menggunakan kebijakan IAM yang berbeda. Dua persona dalam Audit Manager dan kebijakan yang direkomendasikan didefinisikan sebagai berikut.

Persona	Deskripsi dan kebijakan yang direkomendasikan
Pemilik audit	- Persona ini harus memiliki izin yang diperlukan untuk mengelola penilaian di AWS Audit Manager. - Kebijakan yang disarankan untuk digunakan untuk persona ini adalah kebijakan terkelola bernama AWSAuditManagerAdministratorAccess. Anda dapat menggunakan kebijakan ini sebagai titik awal, dan menguraikan izin ini sesuai kebutuhan Anda.
Delegasi	- Persona ini dapat mengakses set kontrol yang didelegasikan dalam penilaian. Mereka dapat memperbarui status kontrol, menambahkan komentar, mengirimkan set kontrol untuk ditinjau, dan menambahkan bukti ke laporan penilaian. - Kebijakan yang disarankan untuk digunakan untuk persona ini adalah contoh kebijakan berikut: Izinkan akses manajemen pengguna ke AWS Audit Manager. Anda dapat menggunakan kebijakan ini sebagai titik awal, dan membuat perubahan yang diperlukan agar sesuai dengan kebutuhan Anda.

Identity-based Contoh kebijakan untuk AWS Audit Manager

Untuk melihat contoh kebijakan berbasis identitas Manajer Audit, lihat. [Identity-based Contoh kebijakan untuk AWS Audit Manager](#)

Resource-based kebijakan di dalam AWS Audit Manager

Mendukung kebijakan berbasis sumber daya: Tidak

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai principal dalam kebijakan berbasis sumber daya. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.

Meskipun AWS Audit Manager tidak memungkinkan Anda mengelola kebijakan berbasis sumber daya melalui IAM, layanan secara internal mengimplementasikan dan mengelola kebijakan berbasis sumber daya untuk dua skenario berikut:

- Ketika pemilik audit ditugaskan untuk penilaian, kebijakan berbasis sumber daya dilampirkan pada penilaian dengan kepala sekolah sebagai pemilik audit. Untuk informasi selengkapnya, lihat [Langkah 3: Tentukan pemilik audit](#) dan [Langkah 3: Edit pemilik audit](#).
- Ketika kumpulan kontrol penilaian didelegasikan, kebijakan berbasis sumber daya dilampirkan ke kumpulan kontrol dengan kepala sekolah sebagai delegasi. Untuk informasi selengkapnya, lihat [Mendelegasikan set kontrol untuk ditinjau AWS Audit Manager](#).

Tindakan kebijakan untuk AWS Audit Manager

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar AWS Audit Manager tindakan, lihat Tindakan yang [ditentukan oleh AWS Audit Manager](#) di Referensi Otorisasi Layanan.

Tindakan kebijakan AWS Audit Manager menggunakan awalan berikut sebelum tindakan.

```
auditmanager
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [
```



```
"auditmanager:GetEvidenceDetails",  
"auditmanager:GetEvidenceEventDetails"  
]
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (*). Misalnya, untuk menentukan semua tindakan yang dimulai dengan kata Get, sertakan tindakan berikut.

```
"Action": "auditmanager:Get*"
```

Untuk melihat contoh kebijakan berbasis identitas Manajer Audit, lihat [Identity-based Contoh kebijakan untuk AWS Audit Manager](#)

Sumber daya kebijakan untuk AWS Audit Manager

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Praktik terbaiknya, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Untuk melihat daftar jenis AWS Audit Manager sumber daya dan ARN-nya, lihat [Sumber Daya yang ditentukan oleh AWS Audit Manager](#) di Referensi Otorisasi Layanan. Untuk mempelajari tentang tindakan yang dapat digunakan untuk menentukan ARN dari setiap sumber daya, lihat [Tindakan yang ditentukan oleh AWS Audit Manager](#).

Penilaian Manajer Audit memiliki format Nama Sumber Daya Amazon (ARN) berikut:

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${assessmentId}
```

Kumpulan kontrol Manajer Audit memiliki format ARN berikut:

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/  
${assessmentId}controlSet/${controlSetId}
```

Kontrol Manajer Audit memiliki format ARN berikut:

```
arn:${Partition}:auditmanager:${Region}:${Account}:control/${controlId}
```

Untuk informasi lebih lanjut tentang format ARN, lihat [Amazon Resource Name \(ARN\)](#).

Misalnya, untuk menentukan `i-1234567890abcdef0` penilaian dalam pernyataan Anda, gunakan ARN berikut.

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/  
i-1234567890abcdef0"
```

Untuk menentukan semua instance milik akun tertentu, gunakan wildcard (*).

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/*"
```

Beberapa tindakan Manajer Audit, seperti untuk membuat sumber daya, tidak dapat dilakukan pada sumber daya tertentu. Dalam kasus tersebut, Anda harus menggunakan wildcard (*).

```
"Resource": ""
```

Banyak tindakan API Manajer Audit melibatkan beberapa sumber daya. Misalnya, `ListAssessments` mengembalikan daftar metadata penilaian yang dapat diakses oleh orang yang saat ini masuk Akun AWS. Oleh karena itu, pengguna harus memiliki izin untuk melihat penilaian. Untuk menentukan beberapa sumber daya dalam satu pernyataan, pisahkan ARN dengan koma.

```
"Resource": [  
    "resource1",  
    "resource2"
```

Untuk melihat daftar jenis sumber daya Audit Manager dan ARN-nya, lihat [Sumber Daya yang Ditetapkan oleh AWS Audit Manager](#) dalam Panduan Pengguna IAM. Untuk mempelajari tentang

tindakan yang dengannya Anda dapat menentukan ARN dari setiap sumber daya, lihat Tindakan yang [Ditetapkan oleh AWS Audit Manager](#).

Beberapa tindakan API Audit Manager mendukung beberapa sumber daya. Misalnya, `GetChangeLogs` mengakses, dan `assessmentID` `controlID` `controlSetId`, jadi kepala sekolah harus memiliki izin untuk mengakses masing-masing sumber daya ini. Untuk menentukan beberapa sumber daya dalam satu pernyataan, pisahkan ARN dengan koma.

```
"Resource": [  
    "assessmentId",  
    "controlId",  
    "controlSetId"
```

Kunci kondisi kebijakan untuk AWS Audit Manager

Mendukung kunci kondisi kebijakan khusus layanan: Sebagian

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan [operator kondisi](#), misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi AND logis. Jika Anda menentukan beberapa nilai untuk kunci kondisi tunggal, AWS mengevaluasi kondisi menggunakan OR operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Jika prinsipal dalam pernyataan kebijakan adalah prinsipal [AWS layanan](#), kami sangat menyarankan Anda menggunakan kunci kondisi [aws:SourceArn](#) atau [aws:SourceAccount](#) global dalam kebijakan. Anda dapat menggunakan kunci konteks kondisi global ini untuk membantu mencegah skenario wakil [yang membingungkan](#). Kebijakan terdokumentasi berikut menunjukkan bagaimana Anda dapat menggunakan kunci konteks kondisi `aws:SourceAccount` global di Audit Manager untuk mencegah masalah wakil yang membingungkan. `aws:SourceArn`

- [Contoh kebijakan untuk topik SNS yang digunakan untuk pemberitahuan Audit Manager](#)

- [Contoh kebijakan untuk kunci KMS yang digunakan dengan topik SNS](#)

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Misalnya, Anda dapat memberikan izin pengguna untuk mengakses sumber daya hanya jika diberi tag dengan nama pengguna mereka. Untuk informasi selengkapnya, lihat [Elemen kebijakan IAM: variabel dan tanda](#) dalam Panduan Pengguna IAM.

Audit Manager tidak menyediakan kunci kondisi khusus layanan apa pun, tetapi mendukung penggunaan beberapa kunci kondisi global. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi [AWS global](#) di Panduan Pengguna IAM.

Daftar kontrol akses (ACL) di AWS Audit Manager

Mendukung ACL: Tidak

Daftar kontrol akses (ACL) mengendalikan principal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Attribute-based kontrol akses (ABAC) dengan AWS Audit Manager

Mendukung ABAC (tanda dalam kebijakan): Ya

Attribute-based kontrol akses (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut yang disebut tag. Anda dapat melampirkan tag ke entitas dan AWS sumber daya IAM, lalu merancang kebijakan ABAC untuk mengizinkan operasi ketika tag kepala sekolah cocok dengan tag pada sumber daya.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di [elemen kondisi](#) dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat [Tentukan izin dengan otorisasi ABAC](#) dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat [Menggunakan kontrol akses berbasis atribut \(ABAC\)](#) dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang menandai AWS Audit Manager sumber daya, lihat [Sumber daya penandaan AWS Audit Manager](#).

Menggunakan kredensial sementara dengan AWS Audit Manager

Mendukung kredensial sementara: Ya

Kredensial sementara menyediakan akses jangka pendek ke AWS sumber daya dan dibuat secara otomatis saat Anda menggunakan federasi atau beralih peran. AWS merekomendasikan agar Anda secara dinamis membuat kredensial sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat [Kredensial keamanan sementara di IAM](#) dan [Layanan AWS yang berfungsi dengan IAM](#) dalam Panduan Pengguna IAM.

Teruskan sesi akses untuk AWS Audit Manager

Mendukung sesi akses terusan (FAS): Ya

Sesi akses maju (FAS) menggunakan izin dari kepala sekolah yang memanggil Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Sesi akses terusan](#).

Peran layanan untuk AWS Audit Manager

Mendukung peran layanan: Tidak

Peran layanan adalah [peran IAM](#) yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS](#) dalam Panduan pengguna IAM.

Warning

Mengubah izin untuk peran layanan dapat merusak fungsionalitas AWS Audit Manager . Edit peran layanan hanya jika Audit Manager memberikan panduan untuk melakukannya.

Service-linked peran untuk AWS Audit Manager

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan dapat mengambil peran untuk melakukan tindakan atas nama Anda. Service-linked peran muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang peran terkait layanan untuk AWS Audit Manager, lihat [Menggunakan peran terkait layanan untuk AWS Audit Manager](#)

Identity-based Contoh kebijakan untuk AWS Audit Manager

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Audit Manager. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat [Membuat kebijakan IAM \(konsol\)](#) di Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh AWS Audit Manager, termasuk format ARN untuk setiap jenis sumber daya, lihat [Tindakan, sumber daya, dan kunci kondisi untuk AWS Audit Manager](#) di Referensi Otorisasi Layanan.

Daftar Isi

- [Praktik terbaik kebijakan](#)
- [Izinkan izin minimum yang diperlukan untuk mengaktifkan Audit Manager](#)
- [Izinkan pengguna akses administrator penuh ke AWS Audit Manager](#)
 - [Contoh 1 \(Kebijakan terkelola, AWSAuditManagerAdministratorAccess\)](#)
 - [Contoh 2 \(Izin tujuan laporan penilaian\)](#)
 - [Contoh 3 \(Izin untuk mengaktifkan pencari bukti\)](#)
 - [Contoh 4 \(Izin untuk menonaktifkan pencari bukti\)](#)
- [Izinkan akses manajemen pengguna ke AWS Audit Manager](#)
- [Izinkan pengguna akses baca-saja ke AWS Audit Manager](#)
- [Mengizinkan pengguna melihat izin mereka sendiri](#)
- [Izinkan AWS Audit Manager untuk mengirim notifikasi ke topik Amazon SNS](#)
 - [Contoh 1 \(Izin untuk topik SNS\)](#)
 - [Contoh 2 \(Izin untuk kunci KMS yang dilampirkan ke topik SNS\)](#)
- [Izinkan pengguna menjalankan kueri pencarian di pencari bukti](#)

Praktik terbaik kebijakan

Identity-based kebijakan menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Pengelola Audit di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa terendah — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan terkel AWS yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat [Kebijakan yang dikelola AWS](#) atau [Kebijakan yang dikelola AWS untuk fungsi tugas](#) dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat [Kebijakan dan izin dalam IAM](#) dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan kondisi untuk memberikan akses ke tindakan layanan jika digunakan melalui tindakan tertentu Layanan AWS, seperti CloudFormation. Untuk informasi selengkapnya, lihat [Elemen kebijakan JSON IAM: Kondisi](#) dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat [Validasi kebijakan dengan IAM Access Analyzer](#) dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) — Jika Anda memiliki skenario yang memerlukan pengguna IAM atau pengguna root Akun AWS, aktifkan MFA untuk keamanan tambahan. Untuk

meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat [Amankan akses API dengan MFA](#) dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat [Praktik terbaik keamanan di IAM](#) dalam Panduan Pengguna IAM.

Izinkan izin minimum yang diperlukan untuk mengaktifkan Audit Manager

Contoh ini menunjukkan bagaimana Anda dapat mengizinkan akun tanpa peran administrator untuk mengaktifkan AWS Audit Manager.

Note

Apa yang kami sediakan di sini adalah kebijakan dasar yang memberikan izin minimum yang diperlukan untuk mengaktifkan Manajer Audit. Semua izin dalam kebijakan berikut ini diperlukan. Jika Anda menghilangkan bagian mana pun dari kebijakan ini, Anda tidak akan dapat mengaktifkan Pengelola Audit.

Kami menyarankan Anda meluangkan waktu untuk menyesuaikan izin Anda sehingga memenuhi kebutuhan spesifik Anda. Jika Anda memerlukan bantuan, hubungi administrator atau Dukungan [AWS Anda](#).

Untuk memberikan akses minimum yang diperlukan untuk mengaktifkan Audit Manager, gunakan izin berikut.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "auditmanager:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
    }
  ]
}
```



```

        "Condition": {
            "StringLike": {
                "iam:AWSServiceName": "auditmanager.amazonaws.com"
            }
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Effect": "Allow",
            "Action": "kms:ListAliases",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        }
    ]
}

```

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai alternatif, hanya izinkan akses ke tindakan yang cocok dengan operasi API yang sedang Anda coba lakukan.

Izinkan pengguna akses administrator penuh ke AWS Audit Manager

Kebijakan contoh berikut memberikan akses administrator penuh ke AWS Audit Manager.

- [Contoh 1 \(Kebijakan terkelola, **AWSAuditManagerAdministratorAccess**\)](#)
- [Contoh 2 \(Izin tujuan laporan penilaian\)](#)
- [Contoh 3 \(Izin untuk mengaktifkan pencari bukti\)](#)
- [Contoh 4 \(Izin untuk menonaktifkan pencari bukti\)](#)

Contoh 1 (Kebijakan terkelola, **AWSAuditManagerAdministratorAccess**)

[AWSAuditManagerAdministratorAccess](#) Kebijakan ini mencakup kemampuan untuk mengaktifkan dan menonaktifkan Audit Manager, kemampuan untuk mengubah setelan Audit Manager, dan kemampuan untuk mengelola semua sumber daya Audit Manager seperti penilaian, kerangka kerja, kontrol, dan laporan penilaian.

Contoh 2 (Izin tujuan laporan penilaian)

Kebijakan ini memberi Anda izin untuk mengakses bucket S3 tertentu, dan untuk menambahkan file ke dan menghapus file darinya. Ini memungkinkan Anda untuk menggunakan bucket yang ditentukan sebagai tujuan laporan penilaian di Audit Manager.

Ganti *placeholder text* dengan informasi Anda sendiri. Sertakan bucket S3 yang Anda gunakan sebagai tujuan laporan penilaian dan kunci KMS yang Anda gunakan untuk mengenkripsi laporan penilaian Anda.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
```

```

        "s3:GetObject",
        "s3:ListBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation",
        "s3:PutObjectAcl"
    ],
    "Resource": "arn:aws:s3:::example-s3-destination-bucket/*"
},
{
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "arn:aws:kms:us-west-2:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
}
]
}

```

Contoh 3 (Izin untuk mengaktifkan pencari bukti)

Kebijakan izin berikut diperlukan jika Anda ingin mengaktifkan dan menggunakan fitur pencari bukti. Pernyataan kebijakan ini memungkinkan Audit Manager membuat penyimpanan data CloudTrail peristiwa Lake dan menjalankan kueri penelusuran.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageCloudTrailLakeQueryAccess",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:StartQuery",
                "cloudtrail:DescribeQuery",
                "cloudtrail:GetQueryResults",
                "cloudtrail:CancelQuery"
            ]
        }
    ]
}

```

```

        "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
    },
    {
        "Sid": "ManageCloudTrailLakeAccess",
        "Effect": "Allow",
        "Action": [
            "cloudtrail:CreateEventDataStore"
        ],
        "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
    }
]
}

```

Contoh 4 (Izin untuk menonaktifkan pencari bukti)

Kebijakan contoh ini memberikan izin untuk menonaktifkan fitur pencari bukti di Audit Manager. Ini melibatkan penghapusan penyimpanan data peristiwa yang dibuat saat Anda pertama kali mengaktifkan fitur.

Sebelum Anda menggunakan kebijakan ini, gantilah *placeholder text* dengan informasi Anda sendiri. Anda harus menentukan UUID penyimpanan data peristiwa yang dibuat saat Anda mengaktifkan pencari bukti. Anda dapat mengambil ARN dari penyimpanan data peristiwa dari pengaturan Audit Manager Anda. Untuk informasi selengkapnya, lihat [GetSettings](#) di dalam Referensi API AWS Audit Manager .

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DeleteEventDataStore",
                "cloudtrail:UpdateEventDataStore"
            ],
            "Resource": "arn:aws:cloudtrail:us-  
east-1:111122223333:eventdatastore/EventDataStoreId"
        }
    ]
}

```

```
}
```

Izinkan akses manajemen pengguna ke AWS Audit Manager

Contoh ini menunjukkan bagaimana Anda dapat mengizinkan akses manajemen non-administrator ke AWS Audit Manager.

Kebijakan ini memberikan kemampuan untuk mengelola semua sumber daya Audit Manager (penilaian, kerangka kerja, dan kontrol), tetapi tidak memberikan kemampuan untuk mengaktifkan atau menonaktifkan Manajer Audit atau untuk mengubah setelan Audit Manager.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AuditManagerAccess",
      "Effect": "Allow",
      "Action": [
        "auditmanager:AssociateAssessmentReportEvidenceFolder",
        "auditmanager:BatchAssociateAssessmentReportEvidence",
        "auditmanager:BatchCreateDelegationByAssessment",
        "auditmanager:BatchDeleteDelegationByAssessment",
        "auditmanager:BatchDisassociateAssessmentReportEvidence",
        "auditmanager:BatchImportEvidenceToAssessmentControl",
        "auditmanager:CreateAssessment",
        "auditmanager:CreateAssessmentFramework",
        "auditmanager:CreateAssessmentReport",
        "auditmanager:CreateControl",
        "auditmanager>DeleteControl",
        "auditmanager>DeleteAssessment",
        "auditmanager>DeleteAssessmentFramework",
        "auditmanager>DeleteAssessmentFrameworkShare",
        "auditmanager>DeleteAssessmentReport",
        "auditmanager:DisassociateAssessmentReportEvidenceFolder",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:GetAssessmentFramework",
        "auditmanager:GetControl",
        "auditmanager:GetServicesInScope",
```

```

        "auditmanager:GetSettings",
        "auditmanager:GetAssessmentReportUrl",
        "auditmanager:GetChangeLogs",
        "auditmanager:GetDelegations",
        "auditmanager:GetEvidence",
        "auditmanager:GetEvidenceByEvidenceFolder",
        "auditmanager:GetEvidenceFileUploadUrl",
        "auditmanager:GetEvidenceFolder",
        "auditmanager:GetEvidenceFoldersByAssessment",
        "auditmanager:GetEvidenceFoldersByAssessmentControl",
        "auditmanager:GetInsights",
        "auditmanager:GetInsightsByAssessment",
        "auditmanager:GetOrganizationAdminAccount",
        "auditmanager:ListAssessments",
        "auditmanager:ListAssessmentReports",
        "auditmanager:ListControls",
        "auditmanager:ListKeywordsForDataSource",
        "auditmanager:ListNotifications",
        "auditmanager:ListAssessmentControlInsightsByControlDomain",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessmentFrameworkShareRequests",
        "auditmanager:ListControlDomainInsights",
        "auditmanager:ListControlDomainInsightsByAssessment",
        "auditmanager:ListControlInsightsByControlDomain",
        "auditmanager:ListTagsForResource",
        "auditmanager:StartAssessmentFrameworkShare",
        "auditmanager:TagResource",
        "auditmanager:UntagResource",
        "auditmanager:UpdateControl",
        "auditmanager:UpdateAssessment",
        "auditmanager:UpdateAssessmentControl",
        "auditmanager:UpdateAssessmentControlSetStatus",
        "auditmanager:UpdateAssessmentFramework",
        "auditmanager:UpdateAssessmentFrameworkShare",
        "auditmanager:UpdateAssessmentStatus",
        "auditmanager:ValidateAssessmentReportIntegrity"
    ],
    "Resource": "*"
},
{
    "Sid": "ControlCatalogAccess",
    "Effect": "Allow",
    "Action": [
        "controlcatalog:ListCommonControls",

```

```

"controlcatalog:ListDomains",
"controlcatalog:ListObjectives"
],
"Resource": "*"
},
{
  "Sid": "OrganizationsAccess",
  "Effect": "Allow",
  "Action": [
    "organizations:ListAccountsForParent",
    "organizations:ListAccounts",
    "organizations:DescribeOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:ListParents",
    "organizations:ListChildren"
  ],
  "Resource": "*"
},
{
  "Sid": "IAMAccess",
  "Effect": "Allow",
  "Action": [
    "iam:GetUser",
    "iam:ListUsers",
    "iam:ListRoles"
  ],
  "Resource": "*"
},
{
  "Sid": "S3Access",
  "Effect": "Allow",
  "Action": [
    "s3:ListAllMyBuckets"
  ],
  "Resource": "*"
},
{
  "Sid": "KmsAccess",
  "Effect": "Allow",
  "Action": [
    "kms:DescribeKey",
    "kms:ListKeys",
    "kms:ListAliases"
  ]
}

```

```

    ],
    "Resource": "*"
  },
  {
    "Sid": "SNSAccess",
    "Effect": "Allow",
    "Action": [
      "sns:ListTopics"
    ],
    "Resource": "*"
  },
  {
    "Sid": "TagAccess",
    "Effect": "Allow",
    "Action": [
      "tag:GetResources"
    ],
    "Resource": "*"
  }
]
}

```

Izinkan pengguna akses baca-saja ke AWS Audit Manager

Kebijakan ini memberikan akses baca-saja ke AWS Audit Manager sumber daya seperti penilaian, kerangka kerja, dan kontrol.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AuditManagerAccess",
      "Effect": "Allow",
      "Action": [
        "auditmanager:Get*",
        "auditmanager:List*"
      ],
      "Resource": "*"
    }
  ]
}

```



```
    ]
  }
}
```

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau secara terprogram menggunakan API AWS CLI or AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

```
}
```

Izinkan AWS Audit Manager untuk mengirim notifikasi ke topik Amazon SNS

Kebijakan dalam contoh ini memberikan izin Audit Manager untuk mengirim notifikasi ke topik Amazon SNS yang ada.

- [Contoh 1](#) — Jika Anda ingin menerima pemberitahuan dari Audit Manager, gunakan contoh ini untuk menambahkan izin ke kebijakan akses topik SNS Anda.
- [Contoh 2](#) — Jika topik SNS Anda menggunakan AWS Key Management Service (AWS KMS) untuk enkripsi sisi server (SSE), gunakan contoh ini untuk menambahkan izin ke kebijakan akses kunci KMS.

Dalam kebijakan berikut, kepala sekolah yang mendapatkan izin adalah prinsipal layanan Manajer Audit, yaitu `auditmanager.amazonaws.com`. Jika prinsipal dalam pernyataan kebijakan adalah prinsipal [AWS layanan](#), kami sangat menyarankan Anda menggunakan kunci kondisi [aws:SourceArn](#) atau [aws:SourceAccount](#) global dalam kebijakan. Anda dapat menggunakan kunci konteks kondisi global ini untuk membantu mencegah skenario wakil [yang membingungkan](#).

Contoh 1 (Izin untuk topik SNS)

Pernyataan kebijakan ini memungkinkan Audit Manager untuk menerbitkan peristiwa ke topik SNS yang ditentukan. Setiap permintaan untuk mempublikasikan ke topik SNS yang ditentukan harus memenuhi ketentuan kebijakan.

Sebelum menggunakan kebijakan ini, ganti *placeholder text* dengan informasi Anda sendiri. Perhatikan hal-hal berikut ini:

- Jika Anda menggunakan kunci `aws:SourceArn` kondisi dalam kebijakan ini, nilainya harus berupa ARN sumber daya Pengelola Audit tempat pemberitahuan berasal. Dalam contoh di bawah ini, `aws:SourceArn` menggunakan wildcard (*) untuk ID sumber daya. Hal ini memungkinkan semua permintaan yang berasal dari Audit Manager pada semua sumber daya Audit Manager. Dengan kunci kondisi `aws:SourceArn` global, Anda dapat menggunakan operator `ArnLike` kondisi `StringLike` atau operator. Sebagai praktik terbaik, kami sarankan Anda menggunakannya `ArnLike`.
- Jika Anda menggunakan kunci [aws:SourceAccount](#) kondisi, Anda dapat menggunakan operator `StringEquals` atau `StringLike` kondisi. Sebagai praktik terbaik, kami sarankan Anda menggunakan `StringEquals` untuk menerapkan hak istimewa terkecil.

- Jika Anda menggunakan keduanya `aws:SourceAccount` dan `aws:SourceArn`, nilai akun harus menunjukkan ID akun yang sama.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "AllowAuditManagerToUseSNSTopic",
    "Effect": "Allow",
    "Principal": {
      "Service": "auditmanager.amazonaws.com"
    },
    "Action": "SNS:Publish",
    "Resource": "arn:aws:sns:us-east-1:111122223333:topicName",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      },
      "ArnLike": {
        "aws:SourceArn": "arn:aws:auditmanager:us-east-1:111122223333:*"
      }
    }
  }
}
```

Contoh alternatif berikut hanya menggunakan kunci `aws:SourceArn` kondisi, dengan operator `StringLike` kondisi:

```
"Condition": {
  "StringLike": {
    "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
  }
}
```

Contoh alternatif berikut hanya menggunakan kunci `aws:SourceAccount` kondisi, dengan operator `StringLike` kondisi:

```
"Condition": {
```

```
"StringLike": {  
  "aws:SourceAccount": "accountID"  
}
```

Contoh 2 (Izin untuk kunci KMS yang dilampirkan ke topik SNS)

Pernyataan kebijakan ini memungkinkan Audit Manager menggunakan kunci KMS untuk [menghasilkan kunci data](#) yang digunakan untuk mengenkripsi topik SNS. Setiap permintaan untuk menggunakan kunci KMS untuk operasi yang ditentukan harus memenuhi ketentuan kebijakan.

Sebelum menggunakan kebijakan ini, ganti *placeholder text* dengan informasi Anda sendiri. Perhatikan hal-hal berikut ini:

- Jika Anda menggunakan kunci `aws:SourceArn` kondisi dalam kebijakan ini, nilainya harus berupa ARN sumber daya yang dienkripsi. Misalnya, dalam hal ini, ini adalah topik SNS di akun Anda. Atur nilai ke ARN atau pola ARN dengan karakter wildcard (*). Anda dapat menggunakan operator `StringLike` atau `ArnLike` kondisi dengan kunci `aws:SourceArn` kondisi. Sebagai praktik terbaik, kami sarankan Anda menggunakannya `ArnLike`.
- Jika Anda menggunakan kunci `aws:SourceAccount` kondisi, Anda dapat menggunakan operator `StringEquals` atau `StringLike` kondisi. Sebagai praktik terbaik, kami sarankan Anda menggunakan `StringEquals` untuk menerapkan hak istimewa terkecil. Anda dapat menggunakan `aws:SourceAccount` jika Anda tidak tahu ARN dari topik SNS.
- Jika Anda menggunakan keduanya `aws:SourceAccount` dan `aws:SourceArn`, nilai akun harus menunjukkan ID akun yang sama.

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": {  
    "Sid": "AllowAuditManagerToUseKMSKey",  
    "Effect": "Allow",  
    "Principal": {  
      "Service": "auditmanager.amazonaws.com"  
    },  
    "Action": [  
      "kms:Decrypt",  
      "kms:GenerateDataKey"  
    ]  
  }  
}
```

```

    ],
    "Resource": "arn:aws:kms:us-east-1:123456789012:key/*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      },
      "ArnLike": {
        "aws:SourceArn": "arn:aws:sns:us-east-1:123456789012:topicName"
      }
    }
  }
}

```

Contoh alternatif berikut hanya menggunakan kunci `aws:SourceArn` kondisi, dengan operator `StringLike` kondisi:

```

"Condition": {
  "StringLike": {
    "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
  }
}

```

Contoh alternatif berikut hanya menggunakan kunci `aws:SourceAccount` kondisi, dengan operator `StringLike` kondisi:

```

"Condition": {
  "StringLike": {
    "aws:SourceAccount": "accountID"
  }
}

```

Izinkan pengguna menjalankan kueri pencarian di pencari bukti

Kebijakan berikut memberikan izin untuk melakukan kueri pada CloudTrail penyimpanan data peristiwa Lake. Kebijakan izin ini diperlukan jika Anda ingin menggunakan fitur pencari bukti.

JSON

```

{
  "Version": "2012-10-17",

```

```
"Statement": [
  {
    "Sid": "ManageCloudTrailLakeQueryAccess",
    "Effect": "Allow",
    "Action": [
      "cloudtrail:StartQuery",
      "cloudtrail:DescribeQuery",
      "cloudtrail:GetQueryResults",
      "cloudtrail:CancelQuery"
    ],
    "Resource": "*"
  }
]
```

Cross-service pencegahan wakil yang bingung

Masalah "confused deputy" adalah masalah keamanan di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memengaruhi entitas yang memiliki hak akses lebih tinggi untuk melakukan tindakan. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Cross-service peniruan diri dapat terjadi ketika satu layanan (layanan panggilan) memanggil layanan lain (layanan yang disebut). Layanan panggilan dapat dimanipulasi untuk menggunakan izinnya untuk bertindak pada sumber daya pelanggan lain ketika tidak memiliki izin untuk melakukannya. Untuk mencegah hal ini, Amazon Web Services menyediakan alat yang membantu Anda melindungi data untuk semua layanan dengan prinsipal layanan yang telah diberikan akses ke sumber daya di akun Anda.

Sebaiknya gunakan kunci konteks [aws:SourceArn](#) dan kondisi [aws:SourceAccount](#) global dalam kebijakan sumber daya untuk membatasi izin yang AWS Audit Manager diberikan ke layanan lain untuk akses ke sumber daya Anda.

- Gunakan `aws:SourceArn` jika Anda ingin hanya satu sumber daya yang akan dikaitkan dengan akses lintas layanan. Anda juga dapat menggunakan `aws:SourceArn` dengan wildcard (*) jika Anda ingin menentukan beberapa sumber daya.

Misalnya, Anda dapat menggunakan topik Amazon SNS untuk menerima pemberitahuan aktivitas dari Manajer Audit. Dalam hal ini, dalam kebijakan akses topik SNS Anda, nilai `aws:SourceArn` adalah sumber daya Manajer Audit tempat pemberitahuan berasal. Karena kemungkinan Anda memiliki beberapa sumber daya Audit Manager, sebaiknya gunakan

`aws:SourceArn` dengan wildcard. Ini memungkinkan Anda untuk menentukan semua sumber daya Manajer Audit Anda dalam kebijakan akses topik SNS Anda.

- Gunakan `aws:SourceAccount` jika Anda ingin mengizinkan sumber daya apa pun di akun tersebut dikaitkan dengan penggunaan lintas layanan.
- Jika `aws:SourceArn` nilai tidak berisi ID akun, seperti ARN bucket Amazon S3, Anda harus menggunakan kedua kunci konteks kondisi global untuk membatasi izin.
- Jika Anda menggunakan kedua kondisi tersebut, dan jika nilainya berisi ID akun, `aws:SourceAccount` nilai dan akun dalam `aws:SourceArn` nilai harus menampilkan ID akun yang sama saat digunakan dalam pernyataan kebijakan yang sama. `aws:SourceArn`
- Cara paling efektif untuk melindungi dari masalah "confused deputy" adalah dengan menggunakan kunci konteks kondisi global `aws:SourceArn` dengan ARN lengkap sumber daya. Jika Anda tidak mengetahui Nama Sumber Daya Amazon (ARN) lengkap dari sumber daya atau jika Anda menentukan beberapa sumber daya, gunakan kunci kondisi konteks `aws:SourceArn` global dengan karakter wildcard (*) untuk bagian ARN yang tidak diketahui. Misalnya, `arn:aws:servicename:*:123456789012:*`.

Manajer Audit bingung dukungan wakil

Manajer Audit memberikan dukungan wakil yang membingungkan dalam skenario berikut. Contoh kebijakan ini menunjukkan bagaimana Anda dapat menggunakan kunci `aws:SourceArn` dan `aws:SourceAccount` kondisi untuk mencegah masalah wakil yang membingungkan.

- [Contoh kebijakan: Topik SNS yang Anda gunakan untuk menerima pemberitahuan Audit Manager](#)
- [Contoh kebijakan: Kunci KMS yang Anda gunakan untuk mengenkripsi topik SNS Anda](#)

Manajer Audit tidak memberikan dukungan wakil yang membingungkan untuk kunci yang dikelola pelanggan yang Anda berikan di [Mengkonfigurasi pengaturan enkripsi data Anda](#) setelah Manajer Audit Anda. Jika Anda memberikan kunci yang dikelola pelanggan Anda sendiri, Anda tidak dapat menggunakan `aws:SourceAccount` atau `aws:SourceArn` ketentuan dalam kebijakan kunci KMS tersebut.

Resource-based Contoh kebijakan untuk AWS Audit Manager

Kebijakan bucket Amazon S3

Kebijakan berikut memungkinkan CloudTrail untuk mengirimkan hasil kueri pencari bukti ke bucket S3 yang ditentukan. Sebagai praktik terbaik keamanan, kunci kondisi global IAM `aws:SourceArn` membantu memastikan bahwa CloudTrail menulis ke bucket S3 hanya untuk penyimpanan data peristiwa.

Important

Anda harus menentukan bucket S3 untuk pengiriman hasil kueri CloudTrail Lake. Untuk informasi selengkapnya, lihat [Menentukan bucket yang ada untuk hasil kueri CloudTrail Lake](#).

Ganti *placeholder text* dengan informasi Anda sendiri, sebagai berikut:

- Ganti *amzn-s3-demo-destination-bucket* dengan bucket S3 yang Anda gunakan sebagai tujuan ekspor.
- Ganti *myQueryRunningRegion* dengan yang sesuai Wilayah AWS untuk konfigurasi Anda.
- Ganti *myAccountID* dengan Akun AWS ID yang digunakan untuk CloudTrail. Ini mungkin tidak sama dengan Akun AWS ID untuk bucket S3. Jika ini adalah penyimpanan data acara organisasi, Anda harus menggunakan Akun AWS untuk akun manajemen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": [
        "s3:PutObject*",
        "s3:Abort*"
      ]
    }
  ]
}
```



```

    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket",
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    ],
    "Condition": {
        "StringEquals": {
            "aws:SourceArn":
"arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
        }
    }
},
{
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
    },
    "Action": "s3:GetBucketAcl",
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
    "Condition": {
        "StringEquals": {
            "aws:SourceArn":
"arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
        }
    }
}
]
}

```

AWS Key Management Service kebijakan

Jika bucket S3 Anda memiliki enkripsi default yang diset SSE-KMS el ke, berikan akses ke CloudTrail dalam kebijakan sumber daya AWS Key Management Service kunci Anda sehingga dapat menggunakan kunci tersebut. Dalam hal ini, tambahkan kebijakan sumber daya berikut ke AWS KMS kunci.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [

```

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt*",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Principal": {
    "Service": "s3.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt*",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*"
}
]
```

AWS kebijakan yang dikelola untuk AWS Audit Manager

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS kebijakan terkelola dirancang untuk memberikan izin untuk banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan ter AWS kelola mungkin tidak memberikan izin hak istimewa terkecil untuk kasus penggunaan spesifik Anda karena kebijakan tersebut tersedia untuk digunakan semua AWS pelanggan. Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan [kebijakan yang dikelola pelanggan](#) yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan ter AWS kelola ketika yang baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat [Kebijakan terkelola AWS](#) dalam Panduan Pengguna IAM.

Topik

- [AWS kebijakan yang dikelola: AWSAuditManagerAdministratorAccess](#)
- [AWS kebijakan yang dikelola: AWSAuditManagerServiceRolePolicy](#)
- [AWS Audit Manager update ke AWS kebijakan terkelola](#)

AWS kebijakan yang dikelola: AWSAuditManagerAdministratorAccess

Anda dapat melampirkan kebijakan `AWSAuditManagerAdministratorAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin administratif yang memungkinkan akses administrasi penuh ke AWS Audit Manager. Akses ini mencakup kemampuan untuk mengaktifkan dan menonaktifkan AWS Audit Manager, mengubah pengaturan AWS Audit Manager, dan mengelola semua sumber daya Audit Manager seperti penilaian, kerangka kerja, kontrol, dan laporan penilaian.

AWS Audit Manager membutuhkan izin luas di beberapa AWS layanan. Ini karena AWS Audit Manager terintegrasi dengan beberapa AWS layanan untuk mengumpulkan bukti secara otomatis dari Akun AWS dan layanan dalam lingkup penilaian.

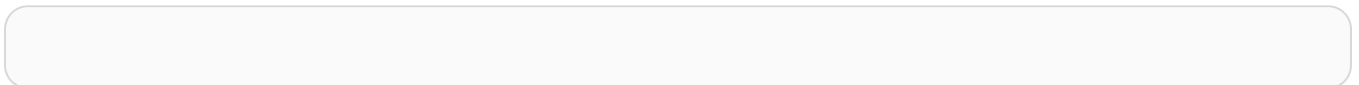
Detail izin

Kebijakan ini mencakup izin berikut:

- `Audit Manager`- Memungkinkan kepala sekolah izin penuh pada AWS Audit Manager sumber daya.
- `Organizations`- Memungkinkan kepala sekolah untuk membuat daftar akun dan unit organisasi, dan untuk mendaftarkan atau membatalkan pendaftaran administrator yang didelegasikan. Ini diperlukan agar Anda dapat mengaktifkan dukungan multi-akun dan memungkinkan AWS Audit Manager untuk menjalankan penilaian di beberapa akun dan mengkonsolidasikan bukti ke dalam akun administrator yang didelegasikan.
- `iam`- Memungkinkan kepala sekolah untuk mendapatkan dan membuat daftar pengguna di IAM dan membuat peran terkait layanan. Ini diperlukan agar Anda dapat menunjuk pemilik audit dan delegasi untuk penilaian. Kebijakan ini juga memungkinkan kepala sekolah untuk menghapus peran terkait layanan dan mengambil status penghapusan. Ini diperlukan agar AWS Audit Manager dapat membersihkan sumber daya dan menghapus peran terkait layanan untuk Anda ketika Anda memilih untuk menonaktifkan layanan di Konsol Manajemen AWS

- `s3`- Memungkinkan kepala sekolah untuk membuat daftar bucket Amazon Simple Storage Service (Amazon S3) yang tersedia. Kemampuan ini diperlukan agar Anda dapat menetapkan bucket S3 tempat Anda ingin menyimpan laporan bukti atau mengunggah bukti manual.
- `kms`- Memungkinkan kepala sekolah untuk membuat daftar dan menjelaskan kunci, daftar alias, dan membuat hibah. Ini diperlukan agar Anda dapat memilih kunci yang dikelola pelanggan untuk enkripsi data.
- `sns`— Memungkinkan kepala sekolah untuk mencantumkan topik berlangganan di Amazon SNS. Ini diperlukan agar Anda dapat menentukan topik SNS mana yang AWS Audit Manager ingin Anda kirim notifikasi.
- `events`- Memungkinkan kepala sekolah untuk membuat daftar dan mengelola cek dari AWS Security Hub CSPM. Hal ini diperlukan agar AWS Audit Manager dapat secara otomatis mengumpulkan AWS Security Hub CSPM temuan untuk AWS layanan yang dipantau oleh AWS Security Hub CSPM. Kemudian dapat mengubah data ini menjadi bukti untuk dimasukkan dalam AWS Audit Manager penilaian Anda.
- `tag`- Memungkinkan kepala sekolah untuk mengambil sumber daya yang ditandai. Ini diperlukan agar Anda dapat menggunakan tag sebagai filter pencarian saat menelusuri kerangka kerja, kontrol, dan penilaian di AWS Audit Manager.
- `controlcatalog`- Memungkinkan kepala sekolah untuk mencantumkan domain, tujuan, dan kontrol umum yang disediakan oleh Katalog AWS Kontrol. Ini diperlukan agar Anda dapat menggunakan fitur kontrol umum di AWS Audit Manager. Dengan izin ini, Anda dapat melihat daftar kontrol umum di pustaka AWS Audit Manager kontrol, dan memfilter kontrol berdasarkan domain dan tujuan. Anda juga dapat menggunakan kontrol umum sebagai sumber bukti saat membuat kontrol kustom.

JSON



AWS kebijakan yang dikelola: `AWSAuditManagerServiceRolePolicy`

Anda tidak dapat melampirkan `AWSAuditManagerServiceRolePolicy` ke entitas IAM Anda. Kebijakan ini dilampirkan ke peran terkait layanan, `AWSServiceRoleForAuditManager`, yang memungkinkan AWS Audit Manager untuk melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat [Menggunakan peran terkait layanan untuk AWS Audit Manager](#).

Kebijakan izin peran, `AWSAuditManagerServiceRolePolicy`, memungkinkan AWS Audit Manager untuk mengumpulkan bukti otomatis dengan melakukan hal berikut atas nama Anda:

- Kumpulkan data dari sumber data berikut:
 - Acara manajemen dari AWS CloudTrail
 - Pemeriksaan kepatuhan dari Aturan AWS Config
 - Pemeriksaan kepatuhan dari AWS Security Hub CSPM
- Gunakan panggilan API untuk menjelaskan konfigurasi sumber daya Anda untuk berikut ini Layanan AWS.

 Tip

Untuk informasi selengkapnya tentang panggilan API yang digunakan Audit Manager untuk mengumpulkan bukti dari layanan ini, lihat [Panggilan API yang didukung untuk sumber data kontrol kustom](#) dalam panduan ini.

- Amazon API Gateway
- AWS Backup
- Amazon Bedrock
- AWS Certificate Manager
- Amazon CloudFront
- AWS CloudTrail
- Amazon CloudWatch
- CloudWatch Log Amazon
- Kumpulan pengguna Amazon Cognito
- AWS Config
- Amazon Data Firehose
- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2
- Amazon EC2 Auto Scaling

- Amazon Elastic File System
- Layanan Amazon Elastic Kubernetes
- Amazon ElastiCache
- Elastic Load Balancing
- Amazon EMR
- Amazon EventBridge
- Amazon FSx
- Amazon GuardDuty
- AWS Identity and Access Management (IAM)
- Amazon Kinesis
- AWS KMS
- AWS Lambda
- AWS License Manager
- Amazon Managed Streaming untuk Apache Kafka
- OpenSearch Layanan Amazon
- AWS Organizations
- Amazon Relational Database Service
- Amazon Redshift
- Amazon Route 53
- Amazon S3
- Amazon SageMaker AI
- AWS Secrets Manager
- AWS Security Hub CSPM
- Layanan Notifikasi Sederhana Amazon
- Amazon Simple Queue Service
- AWS WAF

Detail izin

~~AWSAuditManagerServiceRolePolicy~~ memungkinkan AWS Audit Manager untuk menyelesaikan AWS kebijakan yang dikelola tindakan berikut pada sumber daya yang ditentukan:

- `acm:GetAccountConfiguration`
- `acm:ListCertificates`
- `apigateway:GET`
- `autoscaling:DescribeAutoScalingGroups`
- `backup:ListBackupPlans`
- `backup:ListRecoveryPointsByResource`
- `bedrock:GetCustomModel`
- `bedrock:GetFoundationModel`
- `bedrock:GetModelCustomizationJob`
- `bedrock:GetModelInvocationLoggingConfiguration`
- `bedrock:ListCustomModels`
- `bedrock:ListFoundationModels`
- `bedrock:ListGuardrails`
- `bedrock:ListModelCustomizationJobs`
- `cloudfront:GetDistribution`
- `cloudfront:GetDistributionConfig`
- `cloudfront:ListDistributions`
- `cloudtrail:DescribeTrails`
- `cloudtrail:GetTrail`
- `cloudtrail:ListTrails`
- `cloudtrail:LookupEvents`
- `cloudwatch:DescribeAlarms`
- `cloudwatch:DescribeAlarmsForMetric`
- `cloudwatch:GetMetricStatistics`
- `cloudwatch:ListMetrics`
- `cognito-idp:DescribeUserPool`
- `config:DescribeConfigRules`
- `config:DescribeDeliveryChannels`

- `config:ListDiscoveredResources`
- `directconnect:DescribeDirectConnectGateways`
- `directconnect:DescribeVirtualGateways`
- `dynamodb:DescribeBackup`
- `dynamodb:DescribeContinuousBackups`
- `dynamodb:DescribeTable`
- `dynamodb:DescribeTableReplicaAutoScaling`
- `dynamodb:ListBackups`
- `dynamodb:ListGlobalTables`
- `dynamodb:ListTables`
- `ec2:DescribeAddresses`
- `ec2:DescribeCustomerGateways`
- `ec2:DescribeEgressOnlyInternetGateways`
- `ec2:DescribeFlowLogs`
- `ec2:DescribeInstanceCreditSpecifications`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`
- `ec2:DescribeInternetGateways`
- `ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations`
- `ec2:DescribeLocalGateways`
- `ec2:DescribeLocalGatewayVirtualInterfaces`
- `ec2:DescribeNatGateways`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSecurityGroupRules`
- `ec2:DescribeSnapshots`
- `ec2:DescribeTransitGateways`
- `ec2:DescribeVolumes`

- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcEndpointConnections`
- `ec2:DescribeVpcEndpointServiceConfigurations`
- `ec2:DescribeVpcPeeringConnections`
- `ec2:DescribeVpcs`
- `ec2:DescribeVpnConnections`
- `ec2:DescribeVpnGateways`
- `ec2:GetEbsDefaultKmsKeyId`
- `ec2:GetEbsEncryptionByDefault`
- `ec2:GetLaunchTemplateData`
- `ecs:DescribeClusters`
- `eks:DescribeAddonVersions`
- `elasticache:DescribeCacheClusters`
- `elasticache:DescribeServiceUpdates`
- `elasticfilesystem:DescribeAccessPoints`
- `elasticfilesystem:DescribeFileSystems`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeSslPolicies`
- `elasticloadbalancing:DescribeTargetGroups`
- `elasticmapreduce:ListClusters`
- `elasticmapreduce:ListSecurityConfigurations`
- `es:DescribeDomains`
- `es:DescribeDomain`
- `es:DescribeDomainConfig`
- `es:ListDomainNames`
- `events:DeleteRule`
- `events:DescribeRule`
- `events:DisableRule`
- `events:EnableRule`

- `events:ListConnections`
- `events:ListEventBuses`
- `events:ListEventSources`
- `events:ListRules`
- `events:ListTargetsByRule`
- `events:PutRule`
- `events:PutTargets`
- `events:RemoveTargets`
- `firehose:ListDeliveryStreams`
- `fsx:DescribeFileSystems`
- `guardduty:ListDetectors`
- `iam:GenerateCredentialReport`
- `iam:GetAccessKeyLastUsed`
- `iam:GetAccountAuthorizationDetails`
- `iam:GetAccountPasswordPolicy`
- `iam:GetAccountSummary`
- `iam:GetCredentialReport`
- `iam:GetGroupPolicy`
- `iam:GetPolicy`
- `iam:GetPolicyVersion`
- `iam:GetRolePolicy`
- `iam:GetUser`
- `iam:GetUserPolicy`
- `iam:ListAccessKeys`
- `iam:ListAttachedGroupPolicies`
- `iam:ListAttachedRolePolicies`
- `iam:ListAttachedUserPolicies`
- `iam:ListEntitiesForPolicy`
- `iam:ListGroupsForUser`

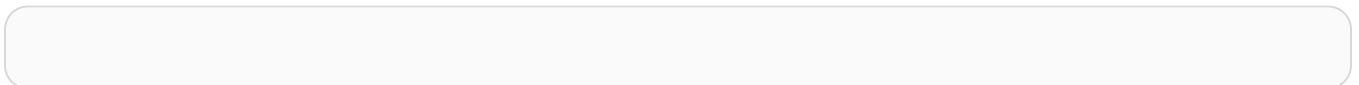
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListMfaDeviceTags
- iam:ListMfaDevices
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListPolicyVersions
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups

- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- logs:GetDataProtectionPolicy
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDBClusterEndpoints
- rds:DescribeDBClusterParameterGroups
- rds:DescribeDBClusters
- rds:DescribeDBInstances
- rds:DescribeDBInstanceAutomatedBackups
- rds:DescribeDBSecurityGroups
- redshift:DescribeClusters
- redshift:DescribeClusterSnapshots
- redshift:DescribeLoggingStatus
- route53:GetQueryLoggingConfig
- s3:GetBucketAcl
- s3:GetBucketLogging
- s3:GetBucketOwnershipControls
- s3:GetBucketPolicy
 - Tindakan API ini beroperasi dalam lingkup di Akun AWS mana peran yang ditautkan layanan tersedia. Itu tidak dapat mengakses kebijakan bucket lintas akun.
- s3:GetBucketPublicAccessBlock
- s3:GetBucketTagging
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3:ListAllMyBuckets

- `sagemaker:DescribeAlgorithm`
- `sagemaker:DescribeDomain`
- `sagemaker:DescribeEndpoint`
- `sagemaker:DescribeEndpointConfig`
- `sagemaker:DescribeFlowDefinition`
- `sagemaker:DescribeHumanTaskUi`
- `sagemaker:DescribeLabelingJob`
- `sagemaker:DescribeModel`
- `sagemaker:DescribeModelBiasJobDefinition`
- `sagemaker:DescribeModelCard`
- `sagemaker:DescribeModelQualityJobDefinition`
- `sagemaker:DescribeTrainingJob`
- `sagemaker:DescribeUserProfile`
- `sagemaker:ListAlgorithms`
- `sagemaker:ListDomains`
- `sagemaker:ListEndpointConfigs`
- `sagemaker:ListEndpoints`
- `sagemaker:ListFlowDefinitions`
- `sagemaker:ListHumanTaskUis`
- `sagemaker:ListLabelingJobs`
- `sagemaker:ListModels`
- `sagemaker:ListModelBiasJobDefinitions`
- `sagemaker:ListModelCards`
- `sagemaker:ListModelQualityJobDefinitions`
- `sagemaker:ListMonitoringAlerts`
- `sagemaker:ListMonitoringSchedules`
- `sagemaker:ListTrainingJobs`
- `sagemaker:ListUserProfiles`
- `securityhub:DescribeStandards`

- `secretsmanager:DescribeSecret`
- `secretsmanager:ListSecrets`
- `sns:ListTagsForResource`
- `sns:ListTopics`
- `sqs:ListQueues`
- `waf-regional:GetLoggingConfiguration`
- `waf-regional:GetRule`
- `waf-regional:GetWebAcl`
- `waf-regional:ListRuleGroups`
- `waf-regional:ListRules`
- `waf-regional:ListSubscribedRuleGroups`
- `waf-regional:ListWebACLs`
- `waf:GetRule`
- `waf:GetRuleGroup`
- `waf:ListActivatedRulesInRuleGroup`
- `waf:ListRuleGroups`
- `waf:ListRules`
- `waf:ListWebAcls`
- `wafv2:ListWebAcls`

JSON



AWS Audit Manager update ke AWS kebijakan terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola AWS Audit Manager sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di [halaman AWS Audit Manager](#) riwayat dokumen.

Ubah	Deskripsi	Tanggal
AWSAuditManagerServiceRolePolicy — Perbaruan ke kebijakan yang sudah ada	Peran terkait layanan sekarang memungkinkan AWS Audit Manager untuk melakukan tindakan. <code>bedrock:ListGuardrails</code> Tindakan API ini diperlukan untuk mendukung AWS Kerangka Praktik Terbaik AI Generatif v2. Ini memungkinkan Manajer Audit untuk mengumpulkan bukti otomatis tentang pagar pembatas yang ada untuk kumpulan data pelatihan data model AI generatif Anda.	09/24/2024
AWSAuditManagerServiceRolePolicy – Pembaruan ke kebijakan yang ada	Kami menambahkan izin berikut ke <code>AWSAuditManagerServiceRolePolicy</code>. AWS Audit Manager sekarang dapat melakukan tindakan berikut untuk mengumpulkan bukti otomatis tentang sumber daya di Akun AWS. • <code>sagemaker:DescribeAlgorithm</code> • <code>sagemaker:DescribeDomain</code> • <code>sagemaker:DescribeEndpoint</code> • <code>sagemaker:DescribeFlowDefinition</code> • <code>sagemaker:DescribeHumanTaskUi</code> • <code>sagemaker:DescribeLabelingJob</code> • <code>sagemaker:DescribeModel</code> • <code>sagemaker:DescribeModelBiasJobDefinition</code> • <code>sagemaker:DescribeModelCard</code> • <code>sagemaker:DescribeModelQualityJobDefinition</code> • <code>sagemaker:DescribeTrainingJob</code> • <code>sagemaker:DescribeUserProfile</code> • <code>sagemaker:ListAlgorithms</code>	06/10/2024

Ubah	Deskripsi	Tanggal
	• sagemaker:ListDomains • sagemaker:ListEndpoints • sagemaker:ListFlowDefinitions • sagemaker:ListHumanTaskUis • sagemaker:ListLabelingJobs • sagemaker:ListModels • sagemaker:ListModelBiasJobDefinitions • sagemaker:ListModelCards • sagemaker:ListModelQualityJobDefinitions • sagemaker:ListMonitoringAlerts • sagemaker:ListMonitoringSchedules • sagemaker:ListTrainingJobs • sagemaker:ListUserProfiles	

Ubah	Deskripsi	Tanggal
AWSAuditManagerServiceRolePolicy – Pembaruan ke kebijakan yang ada	Kami menambahkan izin berikut ke <code>AWSAuditManagerServiceRolePolicy</code>. AWS Audit Manager sekarang dapat melakukan tindakan berikut untuk mengumpulkan bukti otomatis tentang sumber daya di Akun AWS. • <code>iam:ListAttachedGroupPolicies</code> • <code>iam:ListAttachedUserPolicies</code> • <code>iam:ListGroupsForUser</code> • <code>es:ListDomainNames</code> Kami juga menambahkan sumber daya baru di <code>APIGatewayAccess</code> bagian kebijakan (<code>arn:aws:apigateway:*::/restapis</code>). Kebijakan sekarang memberikan izin yang ditentukan (dalam hal ini, <code>apigateway:GET</code> tindakan) tidak hanya pada tahapan dan sumber daya tahap API Gateway REST API, tetapi juga pada REST API itu sendiri. Perubahan ini secara efektif memperluas cakupan kebijakan untuk menyertakan kemampuan untuk mengambil informasi tentang API REST API Gateway itu sendiri, selain sumber daya tahap dan tahap yang terkait dengan API tersebut.	05/17/2024

Ubah	Deskripsi	Tanggal
AWSAuditManagerAdministratorAccess – Pembaruan ke kebijakan yang ada	Kami menambahkan izin berikut ke <code>AWSAuditManagerAdministratorAccess</code> : • <code>controlcatalog:ListCommonControls</code> • <code>controlcatalog:ListDomains</code> • <code>controlcatalog:ListObjectives</code> Pembaruan ini memungkinkan Anda untuk melihat domain kontrol, tujuan kontrol, dan kontrol umum yang disediakan oleh Katalog AWS Kontrol. Izin ini diperlukan jika Anda ingin menggunakan fitur kontrol umum di AWS Audit Manager.	05/15/2024

Ubah	Deskripsi	Tanggal
AWSAuditManagerServiceRolePolicy — Perbarui ke kebijakan yang ada	Kami menambahkan izin berikut ke <code>AWSAuditManagerServiceRolePolicy</code>. AWS Audit Manager sekarang dapat melakukan tindakan berikut untuk mengumpulkan bukti otomatis tentang sumber daya di Akun AWS. • <code>apigateway:GET</code> • <code>autoscaling:DescribeAutoScalingGroups</code> • <code>backup:ListBackupPlans</code> • <code>cloudfront:GetDistribution</code> • <code>cloudfront:GetDistributionConfig</code> • <code>cloudfront:ListDistributions</code> • <code>cloudtrail:GetTrail</code> • <code>cloudtrail:ListTrails</code> • <code>dynamodb:DescribeContinuousBackups</code> • <code>dynamodb:DescribeBackup</code> • <code>dynamodb:DescribeTableReplicaAutoScaling</code> • <code>ec2:DescribeInstanceCreditSpecifications</code> • <code>ec2:DescribeInstanceAttribute</code> • <code>ec2:DescribeSecurityGroupRules</code> • <code>ec2:DescribeVpcEndpointConnections</code> • <code>ec2:DescribeVpcEndpointServiceConfigurations</code> • <code>ec2:GetLaunchTemplateData</code> • <code>es:DescribeDomains</code>	05/15/2024

Ubah	Deskripsi	Tanggal
	• es:DescribeDomain • es:DescribeDomainConfig • iam:GetAccessKeyLastUsed • iam:GetGroupPolicy • iam:GetPolicy • iam:GetPolicyVersion • iam:GetRolePolicy • iam:GetUser • iam:GetUserPolicy • iam:ListAccessKeys • iam:ListAttachedRolePolicies • iam:ListMfaDeviceTags • iam:ListMfaDevices • iam:ListPolicyVersions • logs:GetDataProtectionPolicy • rds:DescribeDBInstanceAutomatedBackups • rds:DescribeDBClusterEndpoints • rds:DescribeDBClusterParameterGroups • redshift:DescribeClusterSnapshots • redshift:DescribeLoggingStatus • s3:GetBucketAcl • s3:GetBucketLogging • s3:GetBucketOwnershipControls • s3:GetBucketTagging • sagemaker:DescribeEndpointConfig • sagemaker:ListEndpointConfigs	

Ubah	Deskripsi	Tanggal
	• <code>secretsmanager:DescribeSecret</code> • <code>secretsmanager:ListSecrets</code> • <code>sns:ListTagsForResource</code> • <code>waf-regional:GetRule</code> • <code>waf-regional:GetWebAcl</code> • <code>waf-regional:ListRules</code> • <code>waf:GetRule</code> • <code>waf:GetRuleGroup</code> • <code>waf:ListRuleGroups</code> • <code>waf:ListRules</code> • <code>waf:ListWebAcls</code> • <code>wafv2:ListWebAcls</code>	
AWSAuditManagerServiceRolePolicy — Perbarui ke kebijakan yang ada	Peran terkait layanan sekarang memungkinkan AWS Audit Manager untuk melakukan tindakan. <code>s3:GetBucketPolicy</code> Tindakan API ini diperlukan untuk mendukung AWS Kerangka Praktik Terbaik AI Generatif v2. Ini memungkinkan Audit Manager mengumpulkan bukti otomatis tentang pembatasan kebijakan yang berlaku untuk kumpulan data pelatihan data model AI generatif Anda. Tindakan <code>GetBucketPolicy</code> beroperasi dalam ruang lingkup di Akun AWS mana peran terkait layanan tersedia. Itu tidak dapat mengakses kebijakan bucket lintas akun.	12/06/2023

Ubah	Deskripsi	Tanggal
AWSAuditManagerServiceRolePolicy — Perbarui ke kebijakan yang ada	Kami menambahkan izin berikut ke <code>AWSAuditManagerServiceRolePolicy</code>. AWS Audit Manager sekarang dapat melakukan tindakan berikut untuk mengumpulkan bukti otomatis tentang sumber daya di Akun AWS. • <code>acm:GetAccountConfiguration</code> • <code>acm:ListCertificates</code> • <code>backup:ListRecoveryPointsByResource</code> • <code>bedrock:GetCustomModel</code> • <code>bedrock:GetFoundationModel</code> • <code>bedrock:GetModelCustomizationJob</code> • <code>bedrock:GetModelInvocationLoggingConfiguration</code> • <code>bedrock:ListCustomModels</code> • <code>bedrock:ListFoundationModels</code> • <code>bedrock:ListModelCustomizationJobs</code> • <code>cloudtrail:LookupEvents</code> • <code>cloudwatch:DescribeAlarmsForMetric</code> • <code>cloudwatch:GetMetricStatistics</code> • <code>cloudwatch:ListMetrics</code> • <code>directconnect:DescribeDirectConnectGateways</code> • <code>directconnect:DescribeVirtualGateways</code> • <code>dynamodb:ListBackups</code> • <code>dynamodb:ListGlobalTables</code>	11/06/2023

Ubah	Deskripsi	Tanggal
	• <code>ec2:DescribeAddresses</code> • <code>ec2:DescribeCustomerGateways</code> • <code>ec2:DescribeEgressOnlyInternetGateways</code> • <code>ec2:DescribeInternetGateways</code> • <code>ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations</code> • <code>ec2:DescribeLocalGateways</code> • <code>ec2:DescribeLocalGatewayVirtualInterfaces</code> • <code>ec2:DescribeNatGateways</code> • <code>ec2:DescribeTransitGateways</code> • <code>ec2:DescribeVpcPeeringConnections</code> • <code>ec2:DescribeVpnConnections</code> • <code>ec2:DescribeVpnGateways</code> • <code>ec2:GetEbsDefaultKmsKeyId</code> • <code>ec2:GetEbsEncryptionByDefault</code> • <code>ecs:DescribeClusters</code> • <code>eks:DescribeAddonVersions</code> • <code>elasticache:DescribeCacheClusters</code> • <code>elasticache:DescribeServiceUpdates</code> • <code>elasticfilesystem:DescribeAccessPoints</code> • <code>elasticloadbalancing:DescribeLoadBalancers</code> • <code>elasticloadbalancing:DescribeSslPolicies</code>	

Ubah	Deskripsi	Tanggal
	• elasticloadbalancing:DescribeTargetGroups • elasticmapreduce:ListClusters • elasticmapreduce:ListSecurityConfigurations • events:ListConnections • events:ListEventBuses • events:ListEventSources • events:ListRules • firehose:ListDeliveryStreams • fsx:DescribeFileSystems • iam:GetAccountPasswordPolicy • iam:GetCredentialReport • iam:ListOpenIdConnectProviders • iam:ListSamlProviders • iam:ListVirtualMFADevices • kafka:ListClusters • kafka:ListKafkaVersions • kinesis:ListStreams • lambda:ListFunctions • logs:DescribeDestinations • logs:DescribeExportTasks • logs:DescribeLogGroups • logs:DescribeMetricFilters • logs:DescribeResourcePolicies • logs:FilterLogEvents • rds:DescribeCertificates • rds:DescribeDbClusterEndpoints	

Ubah	Deskripsi	Tanggal
	• <code>rds:DescribeDbClusterParameterGroups</code> • <code>rds:DescribeDbClusters</code> • <code>rds:DescribeDbSecurityGroups</code> • <code>redshift:DescribeClusters</code> • <code>s3:GetBucketPublicAccessBlock</code> • <code>s3:GetBucketVersioning</code> • <code>sns:ListTopics</code> • <code>sqs:ListQueues</code> • <code>waf-regional:GetLoggingConfiguration</code> • <code>waf-regional:ListRuleGroups</code> • <code>waf-regional:ListSubscribedRuleGroups</code> • <code>waf-regional:ListWebACLs</code>	
AWSAuditManagerServiceRolePolicy — Perbarui ke kebijakan yang ada	Kami menambahkan izin berikut ke <code>AWSAuditManagerServiceRolePolicy</code> : • <code>dynamodb:DescribeTable</code> • <code>dynamodb:ListTables</code> • <code>ec2:DescribeVolumes</code> • <code>kms:GetKeyPolicy</code> • <code>kms:GetKeyRotationStatus</code> • <code>kms:ListKeyPolicies</code> • <code>rds:DescribeDBInstances</code> • <code>redshift:DescribeClusters</code> • <code>s3:GetEncryptionConfiguration</code> • <code>s3:ListAllMyBuckets</code>	07/07/2022

Ubah	Deskripsi	Tanggal
AWSAuditManagerServiceRolePolicy – Pembaruan ke kebijakan yang ada	Peran terkait layanan sekarang memungkinkan AWS Audit Manager untuk melakukan tindakan. <code>organizations:DescribeOrganization</code> Kami juga menguraikan sumber <code>CreateEventsAccess</code> daya dari wildcard (*) ke jenis sumber daya tertentu (<code>arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver</code>). Terakhir, kami menambahkan operator <code>Null</code> kondisi untuk kunci <code>events:source</code> kondisi untuk mengkonfirmasi bahwa nilai sumber ada dan nilainya tidak null.	05/20/2022
AWSAuditManagerAdministratorAccess – Pembaruan ke kebijakan yang ada	Kami memperbarui kebijakan kondisi utama <code>events:source</code> untuk mencerminkan bahwa ini adalah kunci multi-nilai.	04/29/2022
AWSAuditManagerServiceRolePolicy – Pembaruan ke kebijakan yang ada	Kami memperbarui kebijakan kondisi utama <code>events:source</code> untuk mencerminkan bahwa ini adalah kunci multi-nilai.	03/16/2022
AWS Audit Manager mulai melacak perubahan	AWS Audit Manager mulai melacak perubahan untuk kebijakan yang AWS dikelolanya.	05/06/2021

Pemecahan masalah AWS Audit Manager Identitas dan Akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Audit Manager dan IAM.

Topik

- [Saya tidak berwenang untuk melakukan tindakan di AWS Audit Manager](#)
- [Saya tidak berwenang untuk melakukan `iam:PassRole`](#)

- [Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses saya AWS Audit Manager sumber daya](#)

Saya tidak berwenang untuk melakukan tindakan di AWS Audit Manager

Kes `AccessDeniedException` alahan muncul ketika pengguna tidak memiliki izin untuk menggunakan AWS Audit Manager atau operasi API Manajer Audit.

Dalam hal ini, administrator Anda harus memperbarui kebijakan untuk memungkinkan Anda mengakses.

Saya tidak berwenang untuk melakukan `iam:PassRole`

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan tersebut, kebijakan Anda harus diperbarui untuk memungkinkan Anda meneruskan peran ke Manajer Audit.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan itu alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Audit Manager. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses saya AWS Audit Manager sumber daya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang

dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah Audit Manager mendukung fitur-fitur ini, lihat [Bagaimana AWS Audit Manager bekerja dengan IAM](#).
- Untuk mempelajari cara menyediakan akses ke sumber daya di seluruh sumber daya Akun AWS yang Anda miliki, lihat [Menyediakan akses ke pengguna IAM lainnya Akun AWS yang Anda miliki](#) di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat [Menyediakan Akun AWS akan akses milik pihak ketiga](#) di Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat [Menyediakan akses ke pengguna terautentikasi eksternal \(federasi identitas\)](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya [lintas akun di IAM di Panduan Pengguna IAM](#).

Menggunakan peran terkait layanan untuk AWS Audit Manager

AWS Audit Manager menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke Manajer Audit. Service-linked peran telah ditentukan sebelumnya oleh Manajer Audit dan menyertakan semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan AWS Audit Manager lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Manajer Audit mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya Manajer Audit yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat [AWS layanan yang bekerja dengan IAM](#) dan cari layanan yang memiliki Ya di kolom Peran Service-Linked. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Service-linked izin peran untuk AWS Audit Manager

Audit Manager menggunakan peran terkait layanan bernama **AWSServiceRoleForAuditManager**, yang memungkinkan akses ke layanan dan sumber daya AWS yang digunakan atau dikelola oleh AWS Audit Manager.

Peran terkait layanan `AWSServiceRoleForAuditManager` memercayai layanan `auditmanager.amazonaws.com` untuk menjalankan peran.

Kebijakan izin peran, [AWSAuditManagerServiceRolePolicy](#), memungkinkan Audit Manager mengumpulkan bukti otomatis tentang AWS penggunaan Anda. Lebih khusus lagi, ia dapat mengambil tindakan berikut atas nama Anda.

- Audit Manager dapat digunakan AWS Security Hub CSPM untuk mengumpulkan bukti pemeriksaan kepatuhan. Dalam hal ini, Manajer Audit menggunakan izin berikut untuk melaporkan hasil pemeriksaan keamanan langsung dari AWS Security Hub CSPM. Kemudian melampirkan hasil ke kontrol penilaian Anda yang relevan sebagai bukti.
- `securityhub:DescribeStandards`

Note

Untuk informasi selengkapnya tentang kontrol CSPM Hub Keamanan tertentu yang dapat dijelaskan oleh Audit Manager, lihat [AWS Security Hub CSPM kontrol yang didukung oleh AWS Audit Manager](#).

- Audit Manager dapat digunakan AWS Config untuk mengumpulkan bukti pemeriksaan kepatuhan. Dalam hal ini, Audit Manager menggunakan izin berikut untuk melaporkan hasil evaluasi AWS Config aturan langsung dari AWS Config. Kemudian melampirkan hasil ke kontrol penilaian Anda yang relevan sebagai bukti.
- `config:DescribeConfigRules`
- `config:DescribeDeliveryChannels`
- `config:ListDiscoveredResources`

Note

Untuk informasi selengkapnya tentang AWS Config aturan tertentu yang dapat dijelaskan oleh Audit Manager, lihat [AWS Config aturan yang didukung oleh AWS Audit Manager](#).

- Audit Manager dapat digunakan AWS CloudTrail untuk mengumpulkan bukti aktivitas pengguna. Dalam hal ini, Audit Manager menggunakan izin berikut untuk menangkap aktivitas pengguna dari CloudTrail log. Kemudian melampirkan aktivitas ke kontrol penilaian Anda yang relevan sebagai bukti.
- `cloudtrail:DescribeTrails`
- `cloudtrail:LookupEvents`

 Note

Untuk informasi selengkapnya tentang CloudTrail peristiwa tertentu yang dapat dijelaskan oleh Audit Manager, lihat nama [AWS CloudTrail acara yang didukung oleh AWS Audit Manager](#).

- Audit Manager dapat menggunakan panggilan AWS API untuk mengumpulkan bukti konfigurasi sumber daya. Dalam hal ini, Audit Manager menggunakan izin berikut untuk memanggil API read-only yang menjelaskan konfigurasi sumber daya Anda untuk yang berikut ini. Layanan AWS Kemudian melampirkan tanggapan API ke kontrol penilaian Anda yang relevan sebagai bukti.
- `acm:GetAccountConfiguration`
- `acm:ListCertificates`
- `apigateway:GET`
- `autoscaling:DescribeAutoScalingGroups`
- `backup:ListBackupPlans`
- `backup:ListRecoveryPointsByResource`
- `bedrock:GetCustomModel`
- `bedrock:GetFoundationModel`
- `bedrock:GetModelCustomizationJob`
- `bedrock:GetModelInvocationLoggingConfiguration`
- `bedrock:ListCustomModels`
- `bedrock:ListFoundationModels`
- `bedrock:ListGuardrails`
- `bedrock:ListModelCustomizationJobs`
- `cloudfront:GetDistribution`
- `cloudfront:GetDistributionConfig`

- `cloudfront:ListDistributions`
- `cloudtrail:DescribeTrails`
- `cloudtrail:GetTrail`
- `cloudtrail:ListTrails`
- `cloudtrail:LookupEvents`
- `cloudwatch:DescribeAlarms`
- `cloudwatch:DescribeAlarmsForMetric`
- `cloudwatch:GetMetricStatistics`
- `cloudwatch:ListMetrics`
- `cognito-idp:DescribeUserPool`
- `config:DescribeConfigRules`
- `config:DescribeDeliveryChannels`
- `config:ListDiscoveredResources`
- `directconnect:DescribeDirectConnectGateways`
- `directconnect:DescribeVirtualGateways`
- `dynamodb:DescribeBackup`
- `dynamodb:DescribeContinuousBackups`
- `dynamodb:DescribeTable`
- `dynamodb:DescribeTableReplicaAutoScaling`
- `dynamodb:ListBackups`
- `dynamodb:ListGlobalTables`
- `dynamodb:ListTables`
- `ec2:DescribeAddresses`
- `ec2:DescribeCustomerGateways`
- `ec2:DescribeEgressOnlyInternetGateways`
- `ec2:DescribeFlowLogs`
- `ec2:DescribeInstanceCreditSpecifications`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`
- `ec2:DescribeInternetGateways`

- `ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations`
- `ec2:DescribeLocalGateways`
- `ec2:DescribeLocalGatewayVirtualInterfaces`
- `ec2:DescribeNatGateways`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSecurityGroupRules`
- `ec2:DescribeSnapshots`
- `ec2:DescribeTransitGateways`
- `ec2:DescribeVolumes`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcEndpointConnections`
- `ec2:DescribeVpcEndpointServiceConfigurations`
- `ec2:DescribeVpcPeeringConnections`
- `ec2:DescribeVpcs`
- `ec2:DescribeVpnConnections`
- `ec2:DescribeVpnGateways`
- `ec2:GetEbsDefaultKmsKeyId`
- `ec2:GetEbsEncryptionByDefault`
- `ec2:GetLaunchTemplateData`
- `ecs:DescribeClusters`
- `eks:DescribeAddonVersions`
- `elasticache:DescribeCacheClusters`
- `elasticache:DescribeServiceUpdates`
- `elasticfilesystem:DescribeAccessPoints`
- `elasticfilesystem:DescribeFileSystems`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeSslPolicies`
- `elasticloadbalancing:DescribeTargetGroups`

- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- es:DescribeDomains
- es:DescribeDomain
- es:DescribeDomainConfig
- es:ListDomainNames
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccessKeyLastUsed
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:GetGroupPolicy
- iam:GetPolicy
- iam:GetPolicyVersion

- iam:GetRolePolicy
- iam:GetUser
- iam:GetUserPolicy
- iam:ListAccessKeys
- iam:ListAttachedGroupPolicies
- iam:ListAttachedRolePolicies
- iam:ListAttachedUserPolicies
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListGroupsForUser
- iam:ListMfaDeviceTags
- iam:ListMfaDevices
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListPolicyVersions
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies

- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- logs:GetDataProtectionPolicy
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDBClusterEndpoints
- rds:DescribeDBClusterParameterGroups
- rds:DescribeDBClusters
- rds:DescribeDBInstances
- rds:DescribeDBInstanceAutomatedBackups
- rds:DescribeDBSecurityGroups
- redshift:DescribeClusters
- redshift:DescribeClusterSnapshots
- redshift:DescribeLoggingStatus
- route53:GetQueryLoggingConfig
- s3:GetBucketAcl
- s3:GetBucketLogging
- s3:GetBucketOwnershipControls

• ~~s3:GetBucketPolicy~~

Menggunakan peran teraudit layanan

- Tindakan API ini beroperasi dalam lingkup di Akun AWS mana peran yang ditautkan layanan tersedia. Itu tidak dapat mengakses kebijakan bucket lintas akun.
- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketTagging`
- `s3:GetBucketVersioning`
- `s3:GetEncryptionConfiguration`
- `s3:GetLifecycleConfiguration`
- `s3:ListAllMyBuckets`
- `sagemaker:DescribeAlgorithm`
- `sagemaker:DescribeDomain`
- `sagemaker:DescribeEndpoint`
- `sagemaker:DescribeEndpointConfig`
- `sagemaker:DescribeFlowDefinition`
- `sagemaker:DescribeHumanTaskUi`
- `sagemaker:DescribeLabelingJob`
- `sagemaker:DescribeModel`
- `sagemaker:DescribeModelBiasJobDefinition`
- `sagemaker:DescribeModelCard`
- `sagemaker:DescribeModelQualityJobDefinition`
- `sagemaker:DescribeTrainingJob`
- `sagemaker:DescribeUserProfile`
- `sagemaker:ListAlgorithms`
- `sagemaker:ListDomains`
- `sagemaker:ListEndpointConfigs`
- `sagemaker:ListEndpoints`
- `sagemaker:ListFlowDefinitions`
- `sagemaker:ListHumanTaskUis`
- `sagemaker:ListLabelingJobs`
- `sagemaker:ListModels`
- `sagemaker:ListModelBiasJobDefinitions`

- `sagemaker:ListModelCards`
- `sagemaker:ListModelQualityJobDefinitions`
- `sagemaker:ListMonitoringAlerts`
- `sagemaker:ListMonitoringSchedules`
- `sagemaker:ListTrainingJobs`
- `sagemaker:ListUserProfiles`
- `securityhub:DescribeStandards`
- `secretsmanager:DescribeSecret`
- `secretsmanager:ListSecrets`
- `sns:ListTagsForResource`
- `sns:ListTopics`
- `sqs:ListQueues`
- `waf-regional:GetLoggingConfiguration`
- `waf-regional:GetRule`
- `waf-regional:GetWebAcl`
- `waf-regional:ListRuleGroups`
- `waf-regional:ListRules`
- `waf-regional:ListSubscribedRuleGroups`
- `waf-regional:ListWebACLs`
- `waf:GetRule`
- `waf:GetRuleGroup`
- `waf:ListActivatedRulesInRuleGroup`
- `waf:ListRuleGroups`
- `waf:ListRules`
- `waf:ListWebAcls`
- `wafv2:ListWebAcls`

 Note

Untuk informasi selengkapnya tentang panggilan API tertentu yang dapat dijelaskan oleh Audit Manager, lihat [Panggilan API yang didukung untuk sumber data kontrol kustom](#).

Untuk melihat detail izin lengkap dari peran terkait layanan `AWSServiceRoleForAuditManager`, lihat [AWSAuditManagerServiceRolePolicy](#) di Panduan Referensi Kebijakan Ter AWS kelola.

Anda harus mengonfigurasi izin agar entitas IAM (seperti pengguna, grup, atau peran) dapat membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat izin [Service-linked peran](#) di Panduan Pengguna IAM.

Menciptakan AWS Audit Manager peran yang terhubung dengan layanan

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda mengaktifkan AWS Audit Manager, layanan secara otomatis membuat peran terkait layanan untuk Anda. Anda dapat mengaktifkan Audit Manager dari halaman orientasi Konsol Manajemen AWS, atau melalui API atau AWS CLI. Untuk informasi selengkapnya, lihat [Mengaktifkan AWS Audit Manager](#) di panduan pengguna ini.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda.

Mengedit AWS Audit Manager peran yang terhubung dengan layanan

AWS Audit Manager tidak mengizinkan Anda mengedit peran `AWSServiceRoleForAuditManager` terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat [Mengedit peran terkait layanan](#) dalam Panduan Pengguna IAM.

Untuk mengizinkan entitas IAM mengedit deskripsi peran terkait **`AWSServiceRoleForAuditManager`** layanan

Tambahkan pernyataan berikut ke kebijakan izin untuk entitas IAM yang perlu mengedit deskripsi peran terkait layanan.

```
{
  "Effect": "Allow",
  "Action": [
    "iam:UpdateRoleDescription"
  ],
  "Resource": "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
  "Condition": {"StringLike": {"iam:AWSServiceName": "auditmanager.amazonaws.com"}}
}
```

Menghapus AWS Audit Manager peran yang terhubung dengan layanan

Jika Anda tidak perlu lagi menggunakan Audit Manager, sebaiknya hapus peran `AWSServiceRoleForAuditManager` terkait layanan. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Namun, Anda harus membersihkan peran terkait layanan sebelum Anda dapat menghapusnya.

Membersihkan peran terkait layanan

Sebelum Anda dapat menggunakan IAM untuk menghapus peran terkait layanan Manajer Audit, Anda harus terlebih dahulu mengonfirmasi bahwa peran tersebut tidak memiliki sesi aktif dan menghapus sumber daya apa pun yang digunakan oleh peran tersebut. Untuk melakukannya, pastikan bahwa Audit Manager dideregistrasi di semua Wilayah AWS. Setelah Anda membatalkan pendaftaran, Audit Manager tidak lagi menggunakan peran terkait layanan.

Untuk petunjuk tentang cara membatalkan pendaftaran Manajer Audit, lihat sumber daya berikut:

- [Menonaktifkan AWS Audit Manager](#) dalam panduan ini
- [DeregisterAccount](#) di Referensi API AWS Audit Manager
- [deregister-account](#) di [Referensi untuk](#) AWS CLI AWS Audit Manager

Untuk petunjuk tentang cara menghapus sumber daya Audit Manager secara manual, lihat [Penghapusan data Manajer Audit](#) dalam panduan ini.

Menghapus peran terkait layanan

Anda dapat menghapus peran terkait layanan menggunakan konsol IAM, AWS Command Line Interface (AWS CLI), atau IAM API.

IAM console

Ikuti langkah-langkah berikut untuk menghapus peran terkait layanan di konsol IAM.

Untuk menghapus peran terkait layanan (konsol)

1. Masuk ke Konsol Manajemen AWS dan buka konsol IAM di <https://console.aws.amazon.com/iam/>.
2. Di panel navigasi konsol IAM, pilih Peran. Kemudian pilih kotak centang di sebelah `AWSServiceRoleForAuditManager`, bukan nama atau baris itu sendiri.

3. Di bawah Tindakan akan peran di bagian atas halaman, pilih Hapus.
4. Di kotak dialog konfirmasi, tinjau informasi terakhir yang diakses, yang menunjukkan kapan masing-masing peran yang dipilih terakhir mengakses Layanan AWS. Hal ini membantu Anda mengonfirmasi aktif tidaknya peran tersebut saat ini. Jika Anda ingin melanjutkan, masukkan **AWSServiceRoleForAuditManager** di bidang input teks dan pilih Hapus untuk mengirimkan peran terkait layanan untuk dihapus.
5. Perhatikan notifikasi konsol IAM untuk memantau progres penghapusan peran terkait layanan. Karena penghapusan peran terkait layanan IAM bersifat asinkron, setelah Anda mengirimkan peran tersebut untuk penghapusan, tugas penghapusan dapat berhasil atau gagal. Jika tugas berhasil, maka peran dihapus dari daftar dan pesan sukses muncul di bagian atas halaman.

AWS CLI

Anda dapat menggunakan perintah IAM dari AWS CLI untuk menghapus peran terkait layanan.

Untuk menghapus peran terkait layanan (AWS CLI)

1. Masukkan perintah berikut untuk mencantumkan peran di akun Anda:

```
aws iam get-role --role-name AWSServiceRoleForAuditManager
```

2. Karena peran yang terhubung dengan layanan tidak dapat dihapus jika sedang digunakan atau memiliki sumber daya terkait, Anda harus mengirimkan permintaan penghapusan. Permintaan tersebut dapat ditolak jika syarat-syarat ini tidak terpenuhi. Anda harus menangkap `deletion-task-id` dari tanggapan untuk memeriksa status tugas penghapusan.

Ketik perintah berikut untuk mengirimkan permintaan penghapusan peran yang terhubung dengan layanan:

```
aws iam delete-service-linked-role --role-name AWSServiceRoleForAuditManager
```

3. Gunakan perintah berikut untuk memeriksa status tugas penghapusan:

```
aws iam get-service-linked-role-deletion-status --deletion-task-id deletion-task-id
```


Status tugas penghapusan dapat berupa NOT_STARTED, IN_PROGRESS, SUCCEEDED, atau FAILED. Jika penghapusan gagal, panggilan akan mengembalikan alasan kegagalan panggilan agar Anda dapat memecahkan masalah.

IAM API

Anda dapat menggunakan API IAM untuk menghapus peran terkait layanan.

Untuk menghapus peran terkait layanan (API)

1. Panggil [GetRole](#) untuk mencantumkan peran di akun Anda. Dalam permintaan, tent `AWSServiceRoleForAuditManager` ukan sebagaiRoleName.
2. Karena peran yang terhubung dengan layanan tidak dapat dihapus jika sedang digunakan atau memiliki sumber daya terkait, Anda harus mengirimkan permintaan penghapusan. Permintaan tersebut dapat ditolak jika syarat-syarat ini tidak terpenuhi. Anda harus menangkap `DeletionTaskId` dari tanggapan untuk memeriksa status tugas penghapusan.

Untuk mengirimkan permintaan penghapusan untuk peran terkait layanan, hubungi [DeleteServiceLinkedRole](#). Dalam permintaan, tent `AWSServiceRoleForAuditManager` ukan sebagaiRoleName.

3. Untuk memeriksa status penghapusan, panggil [GetServiceLinkedRoleDeletionStatus](#). Di permintaan tersebut, tentukan `DeletionTaskId`.

Status tugas penghapusan dapat berupa NOT_STARTED, IN_PROGRESS, SUCCEEDED, atau FAILED. Jika penghapusan gagal, panggilan akan mengembalikan alasan kegagalan panggilan agar Anda dapat memecahkan masalah.

Kiat untuk menghapus peran terkait layanan Audit Manager

Proses penghapusan untuk peran terkait layanan Manajer Audit mungkin gagal jika Manajer Audit menggunakan peran atau memiliki sumber daya terkait. Ini dapat terjadi dalam skenario berikut:

1. Akun Anda masih terdaftar dengan Audit Manager di satu atau lebih Wilayah AWS.
2. Akun Anda adalah bagian dari AWS organisasi, dan akun manajemen atau akun administrator yang didelegasikan masih terintegrasi ke Manajer Audit.

Untuk mengatasi masalah penghapusan yang gagal, mulailah dengan memeriksa apakah Anda Akun AWS adalah bagian dari Organisasi. Anda dapat melakukan ini dengan memanggil operasi [DescribeOrganization](#) API, atau dengan menavigasi ke AWS Organizations konsol.

Jika Akun AWS adalah bagian dari sebuah organisasi

1. Gunakan akun manajemen Anda untuk [menghapus administrator yang didelegasikan di Manajer Audit](#) di semua Wilayah AWS tempat Anda menambahkannya.
2. Gunakan akun manajemen Anda untuk mem [batalkan pendaftaran Manajer Audit](#) di semua Wilayah AWS tempat Anda menggunakan layanan.
3. Coba lagi untuk menghapus peran terkait layanan dengan mengikuti langkah-langkah dalam prosedur sebelumnya.

Jika Akun AWS Bukan bagian dari sebuah organisasi

1. Pastikan Anda membatalkan [pendaftaran Audit Manager](#) di semua Wilayah AWS tempat Anda menggunakan layanan.
2. Coba lagi untuk menghapus peran terkait layanan dengan mengikuti langkah-langkah dalam prosedur sebelumnya.

Setelah Anda membatalkan pendaftaran dari Audit Manager, layanan akan berhenti menggunakan peran terkait layanan. Anda kemudian dapat menghapus peran dengan sukses.

Wilayah yang Didukung untuk AWS Audit Manager peran terkait layanan

AWS Audit Manager mendukung penggunaan peran terkait layanan di semua Wilayah AWS tempat layanan tersedia. Untuk informasi selengkapnya, lihat [AWS titik akhir layanan](#).

Validasi kepatuhan untuk AWS Audit Manager

Pengalaman AWS pendaftaran baru kami tidak dirancang untuk beban kerja yang diatur. Jika Anda menggunakan pengalaman AWS pendaftaran baru kami, tetapi ingin menggunakannya AWS untuk beban kerja yang diatur, Anda dapat [mendaftar untuk AWS \(lanjutan\)](#) atau [mengaktifkan fitur lanjutan](#) untuk lingkungan Anda AWS .

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat [Layanan AWS di Lingkup berdasarkan Program Kepatuhan](#) dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program Kep [AWS atuhan Program Jaminan](#) .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat [Mengunduh Laporan di AWS Artifact](#).

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. Untuk informasi selengkapnya tentang tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS, lihat Dokumentasi [AWS Keamanan](#).

Memahami ketahanan dalam AWS Audit Manager

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Zona Ketersediaan. Wilayah AWS menyediakan beberapa Zona Ketersediaan yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan.

Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Zona Ketersediaan, lihat Infrastruktur [AWS Global](#).

Keamanan infrastruktur di AWS Audit Manager

Sebagai layanan terkelola, AWS Audit Manager dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat [AWS Keamanan Cloud](#). Untuk merancang AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infra [struktur](#) di Security Pillar AWS Well-Architected Framework.

Anda menggunakan panggilan API yang di AWS publikasikan untuk mengakses AWS Audit Manager melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Suite Cipher dengan kerahasiaan maju sempurna (PFS) seperti DHE (Ephemeral) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Anda dapat memanggil operasi API ini dari lokasi jaringan mana pun, AWS Audit Manager tetapi mendukung kebijakan akses berbasis sumber daya, yang dapat mencakup pembatasan berdasarkan alamat IP sumber. Anda juga dapat menggunakan kebijakan Audit Manager untuk mengontrol akses dari titik akhir Amazon Virtual Private Cloud (Amazon VPC) tertentu atau VPC tertentu. Secara efektif, ini mengisolasi akses jaringan ke sumber daya Audit Manager tertentu dari hanya VPC tertentu dalam jaringan. AWS

AWS Audit Manager dan antarmuka titik akhir VPC (AWS PrivateLink)

Anda dapat membuat koneksi pribadi antara VPC Anda dan AWS Audit Manager dengan membuat titik akhir VPC antarmuka. Titik akhir antarmuka didukung oleh [AWS PrivateLink](#), teknologi yang memungkinkan Anda mengakses API Audit Manager secara pribadi tanpa gateway internet, perangkat NAT, koneksi VPN, atau koneksi AWS Direct Connect. Instans di VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi dengan API Audit Manager. Lalu lintas antara VPC Anda dan AWS Audit Manager tidak meninggalkan AWS jaringan.

Setiap titik akhir antarmuka diwakili oleh satu atau beberapa [Antarmuka Jaringan Elastis](#) di subnet Anda.

Untuk informasi selengkapnya, lihat [Antarmuka VPC endpoint \(AWS PrivateLink\)](#) dalam Panduan Pengguna Amazon VPC.

Pertimbangan untuk AWS Audit Manager Titik akhir VPC

Sebelum menyiapkan titik akhir VPC antarmuka AWS Audit Manager, pastikan Anda meninjau properti dan batasan titik akhir [Antarmuka](#) di Panduan Pengguna Amazon VPC.

AWS Audit Manager mendukung membuat panggilan ke semua tindakan API dari VPC Anda.

Membuat titik akhir antarmuka VPC untuk AWS Audit Manager

Anda dapat membuat titik akhir VPC untuk AWS Audit Manager layanan menggunakan konsol Amazon VPC atau AWS Command Line Interface (AWS CLI). Untuk informasi selengkapnya, lihat [Membuat titik akhir antarmuka](#) dalam Panduan Pengguna Amazon VPC.

Buat titik akhir VPC untuk AWS Audit Manager menggunakan nama layanan berikut:

- `com.amazonaws.region.auditmanager`

Jika Anda mengaktifkan DNS pribadi untuk titik akhir, Anda dapat membuat permintaan API untuk AWS Audit Manager menggunakan nama DNS default untuk Wilayah, misalnya, `auditmanager.us-east-1.amazonaws.com`.

Untuk informasi selengkapnya, lihat [Mengakses layanan melalui titik akhir antarmuka](#) dalam Panduan Pengguna Amazon VPC.

Membuat kebijakan titik akhir VPC untuk AWS Audit Manager

Anda dapat melampirkan kebijakan titik akhir ke VPC endpoint yang mengendalikan akses ke AWS Audit Manager. Kebijakan titik akhir menentukan informasi berikut:

- Prinsipal yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan.
- Sumber daya yang menjadi target tindakan.

Untuk informasi selengkapnya, lihat [Mengontrol Akses ke Layanan dengan titik akhir VPC](#) dalam Panduan Pengguna Amazon VPC.

Contoh: Kebijakan titik akhir VPC untuk AWS Audit Manager tindakan

Berikut ini adalah contoh kebijakan titik akhir untuk AWS Audit Manager. Saat dilampirkan ke titik akhir, kebijakan ini memberikan akses ke tindakan Manajer Audit yang terdaftar untuk semua prinsipal di semua sumber daya.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "auditmanager:GetAssessment",
        "auditmanager:GetServicesInScope",
        "auditmanager:ListNotifications"
      ],
      "Resource": "*"
    }
  ]
}
```

Pencatatan dan pemantauan di AWS Audit Manager

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja Manajer Audit dan AWS solusi Anda yang lain. AWS menyediakan alat pemantauan berikut untuk menonton Audit Manager, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan otomatis bila sesuai:

- AWS CloudTrail merekam panggilan API dan kejadian terkait yang dilakukan oleh atau atas Akun AWS Anda dan mengirimkan berkas log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun yang memanggil AWS, alamat IP asal panggilan dilakukan, dan waktu panggilan terjadi. Untuk informasi selengkapnya, lihat [Panduan Pengguna AWS CloudTrail](#).
- Amazon EventBridge adalah layanan bus acara tanpa server yang memudahkan untuk menghubungkan aplikasi Anda dengan data dari berbagai sumber. EventBridge memberikan aliran data real-time dari aplikasi Anda sendiri, aplikasi Software-as-a-Service (SaaS), dan AWS layanan serta merutekan data tersebut ke target seperti Lambda. Hal ini memungkinkan Anda memantau kejadian yang terjadi dalam layanan, dan membangun arsitektur yang didorong kejadian. Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna [Amazon](#).

Memantau AWS Audit Manager dengan Amazon EventBridge

Amazon EventBridge membantu Anda mengotomatiskan Layanan AWS dan merespons secara otomatis peristiwa sistem seperti masalah ketersediaan aplikasi atau perubahan sumber daya.

Anda dapat menggunakan EventBridge aturan untuk mendeteksi dan bereaksi terhadap peristiwa Audit Manager. Berdasarkan aturan yang Anda buat, memang EventBridge gil satu atau lebih tindakan target saat peristiwa cocok dengan nilai yang Anda tentukan dalam aturan. Bergantung pada jenis acara, Anda mungkin ingin mengirim notifikasi, menangkap informasi peristiwa, mengambil tindakan korektif, memulai peristiwa, atau mengambil tindakan lain.

Misalnya, Anda dapat mendeteksi setiap kali peristiwa Manajer Audit berikut terjadi di akun Anda:

- Pemilik audit membuat, memperbarui, atau menghapus penilaian
- Pemilik audit mendelegasikan kumpulan kontrol untuk ditinjau
- Seorang delegasi menyelesaikan peninjauan mereka dan mengirimkan set kontrol yang ditinjau kembali kepada pemilik audit
- Pemilik audit memperbarui status kontrol penilaian

Tindakan yang dapat dipicu secara otomatis meliputi hal-hal berikut:

- Gunakan AWS Lambda fungsi untuk meneruskan notifikasi ke saluran Slack.
- Dorong data tentang pemeriksaan ke Amazon Kinesis Data Streams untuk mendukung pemantauan status yang komprehensif dan real-time.
- Kirim topik Amazon Simple Notification Service (Amazon SNS) ke email Anda.
- Dapatkan pemberitahuan dengan tindakan CloudWatch alarm Amazon.

Note

Manajer Audit memberikan acara secara tahan lama. Ini berarti bahwa Audit Manager akan berhasil mencoba mengirimkan acara EventBridge setidaknya sekali. Jika peristiwa tidak dapat disampaikan karena gangguan EventBridge layanan, acara tersebut akan dicoba lagi nanti oleh Manajer Audit hingga 24 jam.

EventBridge contoh format untuk Audit Manager

Kode JSON berikut menunjukkan contoh peristiwa pembuatan penilaian di Audit Manager. Untuk informasi tentang salah satu bidang dalam acara ini, lihat Refer [ensi struktur peristiwa](#).

```
{
  "version": "0",
  "id": "55c5a6f3-6183-3989-49ec-a3c998857644",
  "detail-type": "Assessment Created",
  "source": "aws.auditmanager",
  "account": "11112223333",
  "time": "2023-07-27T00:38:33Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:auditmanager:us-west-2:11112223333:assessment/a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6"
  ],
  "detail": {
    "eventID": "4e939b2f-9429-3141-beec-d640d83ef68e",
    "author": "arn:aws:sts::11112223333:assumed-role/roleName/role-session-name",
    "assessmentTenantId": "11112223333",
    "assessmentName": "myAssessment",
```

```

    "eventTime": 1690418289068,
    "eventName": "CREATE",
    "eventType": "ASSESSMENT",
    "assessmentID": "a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6"
  }
}

```

Prasyarat untuk membuat EventBridge aturan

Sebelum membuat aturan untuk acara Audit Manager, sebaiknya lakukan hal berikut:

- Biasakan diri Anda dengan acara, aturan, dan target di dalamnya EventBridge. Untuk informasi lebih lanjut, lihat [Apa itu Amazon EventBridge?](#) dalam Panduan EventBridge Pengguna Amazon.
- Buat target untuk digunakan dalam aturan acara Anda. Misalnya, Anda dapat membuat topik Amazon SNS sehingga setiap kali peninjauan kumpulan kontrol selesai, Anda akan menerima pesan teks atau email. Untuk informasi selengkapnya, lihat [EventBridge target](#).

Membuat EventBridge aturan untuk Manajer Audit

Ikuti langkah-langkah ini untuk membuat EventBridge aturan yang memicu peristiwa yang dipancarkan oleh Audit Manager. Peristiwa dipancarkan atas dasar upaya terbaik.

Untuk membuat EventBridge aturan untuk Audit Manager

1. Buka EventBridge konsol Amazon di <https://console.aws.amazon.com/events/>.
2. Di panel navigasi, pilih Aturan.
3. Pilih Buat aturan.
4. Pada halaman Define rule detail, masukkan nama dan deskripsi aturan.
5. Pertahankan nilai default untuk bus acara dan tipe Aturan, lalu pilih Berikutnya.
6. Pada halaman Membangun pola acara, untuk Sumber acara, pilih AWS acara atau acara EventBridge mitra.
7. Untuk Metode Pembuatan, pilih Pola kustom (editor JSON).
8. Di bawah Pola peristiwa, tulis pola peristiwa di JSON dan tentukan bidang yang ingin Anda gunakan untuk pencocokan.

Untuk mencocokkan acara Audit Manager, Anda dapat menggunakan pola sederhana berikut:

```
{
```



```
"detail-type": ["Event"]
}
```

Ganti **Event** dengan salah satu nilai yang didukung berikut:

- a. Mas Assessment Created uk untuk mendapatkan notifikasi saat penilaian dibuat.
- b. Mas Assessment Updated uk untuk mendapatkan notifikasi saat penilaian diperbarui.
- c. Mas Assessment Deleted uk untuk mendapatkan notifikasi saat penilaian dihapus.
- d. Masukkan Assessment ControlSet Delegation Created untuk mendapatkan notifikasi saat kumpulan kontrol didelegasikan untuk ditinjau.
- e. Masukkan Assessment ControlSet Reviewed untuk mendapatkan notifikasi saat kumpulan kontrol penilaian ditinjau.
- f. Mas Assessment Control Reviewed uk untuk mendapatkan notifikasi saat kontrol penilaian ditinjau.

 Tip

Tambahkan lebih banyak bidang ke pola acara Anda sesuai kebutuhan. Untuk informasi selengkapnya tentang bidang yang tersedia, lihat [P EventBridge ola acara Amazon](#).

9. Pilih Berikutnya.
10. Pada halaman Pilih target, pilih target yang Anda buat untuk aturan ini, lalu konfigurasi opsi tambahan apa pun yang diperlukan untuk jenis tersebut. Misalnya, jika Anda memilih Amazon SNS, pastikan topik SNS Anda dikonfigurasi dengan benar sehingga Anda akan diberi tahu melalui email atau SMS.

 Tip

Bidang yang ditampilkan bervariasi tergantung pada layanan yang dipilih. Untuk informasi selengkapnya tentang target yang tersedia, lihat [Target tersedia di EventBridge konsol](#).

11. Untuk banyak jenis target, EventBridge perlu izin untuk mengirim acara ke target. Dalam kasus ini, Anda EventBridge dapat membuat peran IAM yang diperlukan agar aturan Anda dapat berjalan.

- a. Untuk membuat IAM role secara otomatis, pilih Buat peran baru untuk sumber daya khusus ini.
 - b. Untuk menggunakan IAM role yang Anda buat sebelumnya, pilih Gunakan peran yang ada.
12. (Opsional) Pilih Tambahkan target lain untuk menambahkan target lain untuk aturan ini.
13. Pilih Berikutnya.
14. (Opsional) Pada halaman Konfigurasi tag, tambahkan tag apa pun lalu pilih Berikutnya.
15. Pada halaman Tinjau dan buat, tinjau pengaturan aturan Anda dan pastikan aturan tersebut memenuhi persyaratan pemantauan acara Anda.
16. Pilih Buat aturan. Aturan Anda sekarang akan memantau peristiwa Manajer Audit dan kemudian mengirimkannya ke target yang Anda tentukan.

Pencatatan log AWS Audit Manager Panggilan API dengan CloudTrail

Audit Manager terintegrasi dengan CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau manajer audit. Layanan AWS CloudTrail menangkap semua panggilan API untuk Audit Manager sebagai peristiwa. Panggilan yang diambil mencakup panggilan dari konsol Audit Manager dan panggilan kode ke operasi API Manajer Audit.

Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk acara untuk Audit Manager. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol di Riwayat acara.

Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Manajer Audit, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan itu dibuat, dan detail tambahan.

Untuk mempelajari selengkap CloudTrail nya, lihat Panduan [AWS CloudTrail Pengguna](#).

Informasi Manajer Audit di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di Audit Manager, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan Layanan AWS peristiwa lain dalam riwayat acara.

Anda dapat melihat, mencari, dan mengunduh acara terbaru di Akun AWS. Untuk informasi lain, lihat [Melihat Peristiwa dengan Riwayat Peristiwa CloudTrail](#).

Untuk catatan peristiwa yang berkelanjutan di Akun AWS, termasuk acara untuk Manajer Audit, buat jejak. Jejak CloudTrail memungkinkan pengiriman file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan.

Selain itu, Anda dapat mengonfigurasi Layanan AWS yang lain untuk menganalisis lebih lanjut dan bertindak berdasarkan data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- [Gambaran Umum untuk Membuat Jejak](#)
- [CloudTrail Layanan dan Integrasi yang Didukung](#)
- [Mengonfigurasi Pemberitahuan Amazon SNS untuk CloudTrail](#)
- [Mener CloudTrail ima File Log dari Beberapa Wilayah](#) dan [M CloudTrail enerima File Log dari Beberapa Akun](#)

Semua tindakan Audit Manager dicatat oleh CloudTrail dan didokumentasikan dalam Refer [AWS Audit Manager ensi API](#). Misalnya, panggilan ke operasi `CreateControl`, `DeleteControl`, dan `UpdateAssessmentFramework` API menghasilkan entri dalam file CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut ini:

- Apakah permintaan dibuat dengan kredensial pengguna root.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan tersebut dibuat oleh Layanan AWS lain.

Untuk informasi lain, lihat [Elemen userIdentity CloudTrail](#).

Memahami Entri File Log Manajer Audit

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah

jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [CreateAssessment](#) tindakan.

```
{
  eventVersion:"1.05",
  userIdentity:{
    type:"IAMUser",
    principalId:"principalId",
    arn:"arn:aws:iam::accountId:user/userName",
    accountId:"111122223333",
    accessKeyId:"accessKeyId",
    userName:"userName",
    sessionContext:{
      sessionIssuer:{
      },
      webIdFederationData:{
      },
      attributes:{
        mfaAuthenticated:"false",
        creationDate:"2020-11-19T07:32:06Z"
      }
    }
  },
  eventTime:"2020-11-19T07:32:36Z",
  eventSource:"auditmanager.amazonaws.com",
  eventName:"CreateAssessment",
  awsRegion:"us-west-2",
  sourceIPAddress:"sourceIPAddress",
  userAgent:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  requestParameters:{
    frameworkId:"frameworkId",
    assessmentReportsDestination:{
      destination:"****",
      destinationType:"S3"
    },
    clientToken:"****",
    scope:{
      awsServices:[
        {
          serviceName:"license-manager"
        }
      ]
    }
  }
}
```

```
    ],
    awsAccounts:"****"
  },
  roles:"****",
  name:"****",
  description:"****",
  tags:"****"
},
responseElements:{
  assessment:"****"
},
requestID:"0d950f8c-5211-40db-8c37-2ed38ffcc894",
eventID:"a782029a-959e-4549-81df-9f6596775cb0",
readOnly:false,
eventType:"AwsApiCall",
recipientAccountId:"recipientAccountId"
}
```

Memahami konfigurasi dan analisis kerentanan di AWS Audit Manager

Konfigurasi dan kontrol TI adalah tanggung jawab bersama antara AWS dan Anda, pelanggan kami. Untuk informasi selengkapnya, lihat model tanggung jawab AWS [bersama](#).

Menonaktifkan AWS Audit Manager

Anda dapat menonaktifkan Audit Manager jika Anda tidak lagi ingin menggunakan layanan. Ketika Anda menonaktifkan Audit Manager, Anda juga memiliki opsi untuk menghapus semua data Anda.

Secara default, data Anda tidak dihapus saat Anda menonaktifkan Audit Manager. Data bukti Anda disimpan selama dua tahun sejak pembuatannya. Sumber daya Audit Manager Anda yang lain (termasuk penilaian, kontrol kustom, dan kerangka kerja kustom) dipertahankan tanpa batas waktu, dan akan tersedia jika Anda mengaktifkan kembali Audit Manager di masa mendatang. Untuk informasi selengkapnya tentang retensi [data, lihat Perlindungan Data](#) dalam panduan ini.

Jika Anda memilih untuk menghapus data, Audit Manager menghapus semua data bukti bersama dengan semua sumber daya Audit Manager yang Anda buat (termasuk penilaian, kontrol kustom, dan kerangka kerja kustom). Semua data Anda dihapus dalam waktu tujuh hari setelah menonaktifkan Audit Manager.

Topik

- [Prosedur](#)
- [Langkah berikutnya](#)
- [Sumber daya tambahan](#)

Prosedur

Anda dapat menonaktifkan Audit Manager menggunakan konsol Audit Manager, AWS Command Line Interface (AWS CLI), atau Audit Manager API.

Warning

- Saat Anda menonaktifkan Audit Manager, akses Anda dicabut dan layanan tidak lagi mengumpulkan bukti untuk penilaian yang ada. Anda tidak dapat mengakses apa pun di layanan kecuali Anda mengaktifkan kembali Audit Manager.
- Menghapus semua data adalah tindakan permanen. Jika Anda memutuskan untuk mengaktifkan kembali Audit Manager di masa mendatang, data Anda tidak akan dapat dipulihkan.

Audit Manager console

Untuk menonaktifkan Audit Manager di konsol Audit Manager

1. Dari tab Pengaturan umum, buka AWS Audit Manager bagian Nonaktifkan.
2. Pilih Disable (Nonaktifkan).
3. Di jendela pop-up, tinjau pengaturan penyimpanan data Anda saat ini.
 - a. Untuk melanjutkan pilihan Anda saat ini, pilih Nonaktifkan Audit Manager.
 - b. Untuk mengubah pilihan Anda saat ini, lakukan langkah-langkah berikut:
 - i. Pilih Batal untuk kembali ke halaman pengaturan.
 - ii. Untuk menggunakan pengaturan penyimpanan data default, matikan Hapus semua data. Seleksi ini menyimpan data bukti selama dua tahun sejak pembuatannya, dan mempertahankan sumber daya Audit Manager lainnya tanpa batas waktu.
 - iii. Untuk menghapus data Anda, aktifkan Hapus semua data.
 - iv. Pilih Nonaktifkan, lalu pilih Nonaktifkan Audit Manager untuk mengonfirmasi pilihan Anda.

AWS CLI

Sebelum Anda mulai

Sebelum menonaktifkan Audit Manager, Anda dapat menjalankan perintah [update-settings](#) untuk menyetel kebijakan penyimpanan data pilihan Anda. Secara default, Audit Manager menyimpan data Anda. Jika Anda ingin meminta penghapusan data Anda, gunakan `--deregistration-policy` parameter dengan `deleteResources` nilai yang disetel ke. ALL

```
aws auditmanager update-settings --deregistration-policy deleteResources=ALL
```

Untuk menonaktifkan Audit Manager di AWS CLI

Saat Anda siap menonaktifkan Audit Manager, jalankan perintah [deregister-account](#).

```
aws auditmanager deregister-account
```

Audit Manager API

Sebelum Anda mulai

Sebelum menonaktifkan Audit Manager, Anda dapat menggunakan operasi [UpdateSettings](#) API untuk menyetel kebijakan penyimpanan data pilihan Anda. Secara default, Audit Manager menyimpan data Anda. Jika Anda ingin menghapus data Anda, Anda dapat menggunakan [DeregistrationPolicy](#) atribut untuk meminta penghapusan data Anda.

Untuk menonaktifkan Audit Manager menggunakan API

Ketika Anda siap untuk menonaktifkan Audit Manager, hubungi [DeregisterAccount](#) operasi.

Untuk informasi selengkapnya, pilih tautan sebelumnya untuk membaca selengkapnya di Referensi API Audit Manager. Ini termasuk informasi tentang cara menggunakan operasi dan parameter ini di salah satu bahasa khusus AWS SDKs.

Langkah berikutnya

Jika Anda perlu mengaktifkan kembali Audit Manager setelah menonaktifkannya, ikuti langkah-langkah berikut untuk mengaktifkan dan menjalankan kembali layanan.

Untuk mengaktifkan kembali Audit Manager setelah Anda menonaktifkannya

Buka beranda layanan Audit Manager dan ikuti langkah-langkah untuk mengatur Audit Manager sebagai pengguna baru. Untuk informasi selengkapnya, lihat [Pengaturan AWS Audit Manager dengan pengaturan yang disarankan](#).

Tip

- Jika Anda memilih untuk menghapus data saat menonaktifkan Audit Manager, Anda harus menunggu hingga data dihapus sebelum dapat mengaktifkan kembali layanan. Tergantung pada berapa banyak data yang Anda miliki, ini bisa memakan waktu hingga tujuh hari. Namun, jangan ragu untuk mencoba mengaktifkan kembali Audit Manager sebelum itu. Dalam banyak kasus, data dihapus hanya dalam satu jam.
- Jika Anda memilih untuk tidak menghapus data saat Anda menonaktifkan Audit Manager, penilaian yang ada dipindahkan ke keadaan tidak aktif dan berhenti mengumpulkan bukti sebagai hasilnya. Untuk mulai mengumpulkan bukti lagi untuk penilaian yang sudah ada sebelumnya, [edit penilaian](#) dan pilih Simpan tanpa membuat perubahan apa pun.

Sumber daya tambahan

- Untuk informasi selengkapnya tentang retensi data di Audit Manager, lihat [Perlindungan Data](#) dalam panduan ini.

Riwayat dokumen untuk AWS Audit Manager Panduan Pengguna

Tabel berikut menjelaskan perubahan penting dalam setiap rilis Panduan AWS Audit Manager Pengguna mulai 8 Desember 2020, dan seterusnya.

Perubahan	Deskripsi	Tanggal
AWS Audit Manager Tidak lagi terbuka untuk pelanggan baru.	AWS Audit Manager Tidak lagi terbuka untuk pelanggan baru. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat perubahan AWS Audit Manager ketersediaan .	30 April 2026
AWS Audit Manager tidak akan lagi terbuka untuk pelanggan baru mulai 30 April 2026.	AWS Audit Manager tidak akan lagi terbuka untuk pelanggan baru mulai 30 April 2026. Jika Anda ingin menggunakan Audit Manager, daftar sebelum tanggal tersebut. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat perubahan AWS Audit Manager ketersediaan .	Maret 31, 2026
Pembaruan untuk lima kerangka kerja yang didukung	Kerangka kerja berikut telah diperbarui: • Kontrol Awan Sedang CCCS	Juli 17, 2025

- [ISO/IEC 27001:2013 Lampiran A](#)
- [PCI DSS V3.2.1](#)
- [PCI DSS V4.0](#)
- [SSAE-18 SOC 2](#)

[Pembaruan untuk lima kerangka kerja yang didukung](#)

Kerangka kerja berikut telah diperbarui:

Juni 19, 2025

- [Kerangka Kerja Berarsitektur Baik \(WAF\) Layanan Web Amazon \(AWS\) v10](#)
- [Kontrol Dasar Keamanan FedRAMP r4](#)
- [NIST SP 800-171 Rev 2](#)
- [NIST-CSF-v1.1](#)
- [NIST-SP-800-53-r5](#)

[Pembaruan untuk tiga kerangka kerja yang didukung](#)

Kerangka kerja berikut telah diperbarui:

Juni 4, 2025

- [ACSC Esensial Delapan](#)
- [ACSC ISM](#)
- [Kontrol Keamanan Kritis CIS versi 8.0, IG1](#)

[Diperbarui kerangka kerja yang didukung: CIS Controls v7.1, IG1](#)

CIS Controls v7.1, kerangka kerja IG1 telah diperbarui. Untuk informasi selengkapnya, lihat [Kontrol CIS v7.1, IG 1](#).

Mei 14, 2025

[Kebijakan s3_ yang ListBuckets diperbarui](#)

AWS Audit Manager telah memperbarui s3_ListBuckets kebijakan dan dokumentasi agar s3_GetBucketEncryption sesuai dengan kebijakan. Untuk informasi selengkapnya, lihat [Panggilan API yang didukung untuk sumber data kontrol kustom.](#)

Maret 24, 2025

[Kebijakan ter AWS kelola yang diperbarui](#)

AWS Audit Manager telah memperbarui [AWSAuditManagerServiceRolePolicy](#). Untuk informasi selengkapnya, lihat kebijakan [AWS terkelola untuk AWS Audit Manager](#).

September 24, 2024

[Kerangka kerja baru yang didukung: praktik terbaik AI AWS generatif v2](#)

Kerangka kerja bawaan baru sekarang tersedia di AWS Audit Manager. Untuk informasi selengkapnya, lihat kerangka kerja praktik terbaik AI [AWS generatif v2](#).

Juni 11, 2024

[Kebijakan ter AWS kelola yang diperbarui](#)

AWS Audit Manager telah memperbarui [AWSAuditManagerServiceRolePolicy](#). Untuk informasi selengkapnya, lihat kebijakan [AWS terkelola untuk AWS Audit Manager](#).

Juni 10, 2024

[Gunakan kontrol umum untuk menyederhanakan cara Anda menjalankan penilaian terhadap kontrol perusahaan](#)

Saat Anda membuat kontrol kustom, Anda sekarang dapat menggunakan kontrol umum sebagai sumber bukti. Setiap kontrol umum memetakan ke pengelompokan sumber AWS data yang relevan yang dikelola. Pengelompokan yang telah ditentukan sebelumnya ini merampingkan pengumpulan bukti dengan menghilangkan kebutuhan untuk mengidentifikasi AWS sumber daya mana yang perlu dinilai untuk kontrol tertentu. Untuk informasi tentang cara menemukan kontrol umum dan menggunakannya sebagai sumber bukti, lihat Pust [aka kontrol](#).

Juni 6, 2024

[Kebijakan ter AWS kelola yang diperbarui](#)

AWS Audit Manager telah memperbarui [AWSAuditManagerServiceRolePolicy](#). Untuk informasi selengkapnya, lihat kebijakan [AWS terkelola untuk AWS Audit Manager](#).

17 Mei 2024

[Kebijakan ter AWS kelola yang diperbarui](#)

AWS Audit Manager telah memperbarui [AWSAuditManagerAdministratorAccess](#) kebijakan. Untuk informasi selengkapnya, lihat kebijakan [AWS terkelola untuk AWS Audit Manager](#).

Mei 15, 2024

[Kebijakan ter AWS kelola yang diperbarui](#)

AWS Audit Manager telah memperbarui [AWSAuditManagerServiceRolePolicy](#). Untuk informasi selengkapnya, lihat kebijakan [AWS terkelola untuk AWS Audit Manager](#).

Mei 15, 2024

[Dukungan untuk panggilan AWS API tambahan](#)

Anda sekarang dapat menggunakan panggilan AWS API tambahan sebagai sumber data untuk kontrol kustom Anda di Audit Manager. Untuk informasi selengkapnya, lihat [Panggilan API yang didukung untuk sumber data kontrol kustom](#).

Mei 15, 2024

[Kerangka kerja baru yang didukung: PCI DSS V4.0](#)

Kerangka kerja bawaan baru sekarang tersedia di AWS Audit Manager. Untuk informasi lain, lihat [PCI DSS V4.0](#).

Desember 19, 2023

[Dukungan untuk panggilan AWS API tambahan](#)

Anda sekarang dapat menggunakan panggilan AWS API tambahan sebagai sumber data untuk kontrol kustom Anda di Audit Manager. Untuk informasi selengkapnya, lihat [Panggilan API yang didukung untuk sumber data kontrol kustom](#).

Desember 7, 2023

Kebijakan ter AWS kelola yang diperbarui	AWS Audit Manager telah memperbarui AWSAuditManagerServiceRolePolicy. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Audit Manager.	6 Desember 2023
Dukungan untuk temuan kontrol AWS Security Hub CSPM konsolidasi	Manajer Audit sekarang mendukung kontrol konsolidasi di AWS Security Hub CSPM. Untuk informasi selengkapnya, lihat AWS Security Hub CSPM kontrol yang didukung oleh AWS Audit Manager.	16 November 2023
Integrasi dengan MetricStream	Anda sekarang dapat menelan bukti dari Manajer Audit ke MetricStream. Untuk informasi selengkapnya, lihat Integrasi dengan produk GRC pihak ketiga.	14 November 2023
Kerangka kerja baru yang didukung: AWS praktik terbaik AI generatif	Kerangka kerja bawaan baru sekarang tersedia di AWS Audit Manager. Untuk informasi selengkapnya, lihat kerangka kerja praktik terbaik AI AWS generatif v1.	8 November 2023
Kebijakan ter AWS kelola yang diperbarui	AWS Audit Manager telah memperbarui AWSAuditManagerServiceRolePolicy. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Audit Manager.	6 November 2023

[Integrasi dengan Amazon EventBridge](#)

Anda sekarang dapat memantau peristiwa yang terjadi di AWS Audit Manager dan menggunakan peristiwa ini sebagai bagian dari arsitektur berbasis peristiwa Anda. Untuk informasi selengkapnya, lihat [Pemantauan AWS Audit Manager dengan Amazon EventBridge](#).

18 Agustus 2023

[Dukungan untuk penilaian risiko dan opsi bukti manual baru](#)

Anda sekarang dapat menggunakan alur kerja pembuatan kontrol kustom untuk mendukung penilaian risiko. Kontrol sekarang dapat mewakili pertanyaan penilaian risiko, dan Anda dapat memberikan jawaban dengan mengunggah file atau memasukkan teks sebagai bukti manual. Untuk informasi selengkapnya, lihat [Membuat kontrol kustom](#) dan [Menambahkan bukti manual](#).

12 Juni 2023

[Dukungan untuk ekspor CSV](#)

Anda sekarang dapat mengekspor hasil pencarian pencari bukti Anda dalam format CSV. Untuk informasi selengkapnya, lihat [Meng ekspor hasil penelusuran Anda](#).

9 Juni 2023

[Kerangka kerja baru yang didukung: Manual Keamanan Informasi Pusat Keamanan Cyber Australia \(ACSC\)](#)

Kerangka kerja bawaan baru sekarang tersedia di AWS Audit Manager. Untuk informasi lebih lanjut, lihat Manual [Keamanan Informasi Pusat Keamanan Cyber Australia \(ACSC\)](#).

24 Maret 2023

[Laporan penilaian yang ditingkatkan](#)

Kami melakukan perbaikan pada format dan isi laporan penilaian Manajer Audit. Untuk informasi selengkapnya tentang cara menavigasi dan memahami laporan penilaian, lihat [Laporan penilaian](#).

Maret 23, 2023

[Dukungan untuk panggilan API berpaginasi](#)

AWS Audit Manager sekarang mendukung panggilan API berpaginasi sebagai sumber data untuk pengumpulan bukti. Untuk informasi selengkapnya, lihat Pang [gilan](#) API berpaginasi.

8 Maret 2023

[Kerangka kerja baru yang didukung: Aturan Keamanan Omnibus Final HIPAA 2013](#)

Kerangka kerja bawaan baru sekarang tersedia di AWS Audit Manager. Untuk informasi selengkapnya, lihat A [aturan Keamanan Omnibus Final HIPAA 2013](#). Untuk tujuan diferensiasi, kerangka kerja HIPAA yang ada sebelumnya (sebelumnya bernama HIPAA di perpustakaan kerangka kerja) sekarang bernama [HIPAA Security Rule 2003](#).

8 Maret 2023

[Dukungan untuk panggilan
AWS API tambahan](#)

Anda sekarang dapat menggunakan sembilan panggilan AWS API tambahan sebagai sumber data untuk kontrol kustom Anda di Audit Manager. Untuk informasi selengkapnya, lihat [Panggilan API yang didukung untuk sumber data kontrol kustom](#).

3 Maret 2023

[Panduan yang diperbarui
untuk menyelaraskan dengan
praktik terbaik IAM](#)

Memperbarui panduan untuk menyelaraskan dengan praktik terbaik IAM. Untuk informasi lebih lanjut, lihat [Praktik terbaik keamanan di IAM](#).

Januari 6, 2023

[Pengaturan retensi data baru](#)

Anda sekarang dapat menentukan apakah Anda ingin menghapus semua data Anda ketika Anda menonaktifkan Audit Manager. Untuk informasi selengkapnya, lihat [Menonaktifkan AWS Audit Manager](#) dan [Menghapus data Manajer Audit](#).

Januari 6, 2023

[Dukungan untuk pencari bukti](#)

Anda sekarang dapat menggunakan pencari bukti untuk melakukan permintaan pencarian pada data bukti Anda. Untuk informasi selengkapnya, lihat [Pencari bukti](#).

18 November 2022

Kerangka kerja baru yang didukung: Pusat Keamanan Cyber Australia (ACSC) Essential Eight	Kerangka kerja bawaan baru sekarang tersedia di AWS Audit Manager. Untuk informasi lebih lanjut, lihat Pusat Keamanan Cyber Australia (ACSC) Essential Eight .	Agustus 24, 2022
Kebijakan ter AWS kelola yang diperbarui	AWS Audit Manager telah memperbarui AWSAuditManagerServiceRolePolicy . Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Audit Manager .	Juli 7, 2022
Kebijakan ter AWS kelola yang diperbarui	AWS Audit Manager telah memperbarui AWSAuditManagerServiceRolePolicy . Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Audit Manager .	Mei 20, 2022
Kerangka kerja baru yang didukung: Profil Kontrol Cloud Medium Pusat Keamanan Cyber Kanada	Kerangka kerja bawaan baru sekarang tersedia di AWS Audit Manager. Untuk informasi selengkapnya, lihat Profil Kontrol Cloud Medium Pusat Keamanan Cyber Kanada .	6 Mei 2022
Kebijakan ter AWS kelola yang diperbarui	AWS Audit Manager telah memperbarui AWSAuditManagerAdministratorAccess kebijakan. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Audit Manager .	29 April 2022

[Dukungan untuk aturan ter
AWS Config kelola tambahan](#)

Anda sekarang dapat menggunakan 91 aturan terkel AWS Config ola tambahan sebagai sumber data untuk kontrol kustom Anda di Audit Manager. Untuk informasi selengkapnya, lihat [Menggunakan aturan AWS Config terkelola dengan AWS Audit Manager.](#)

27 April 2022

[Dukungan untuk aturan AWS
Config khusus](#)

Anda sekarang dapat menggunakan aturan AWS Config khusus sebagai sumber data untuk kontrol kustom Anda di Audit Manager. Untuk informasi selengkapnya, lihat [Menggunakan aturan AWS Config khusus dengan AWS Audit Manager.](#)

27 April 2022

[Kerangka kerja baru yang
didukung: ISO/IEC 27001:201
3 Lampiran A](#)

Kerangka kerja bawaan baru sekarang tersedia di AWS Audit Manager. Untuk informasi lebih lanjut, lihat [ISO/IEC 27001:2013 Lampiran A.](#)

7 April 2022

[Kebijakan ter AWS kelola yang
diperbarui](#)

AWS Audit Manager telah memperbarui [AWSAuditManagerServiceRolePolicy.](#) Untuk informasi selengkapnya, lihat kebijakan [AWS terkelola untuk AWS Audit Manager.](#)

16 Maret 2022

[Kerangka kerja baru yang didukung: CIS Benchmark untuk CIS Amazon Web Services Foundations Benchmark v1.4](#)

Dua kerangka kerja prebuilt baru sekarang tersedia di AWS Audit Manager: CIS Benchmark untuk CIS Amazon Web Services Foundations Benchmark v1.4, Level 1, dan CIS Benchmark untuk CIS Amazon Web Services Foundations Benchmark v1.4, Level 1 dan 2. Untuk informasi selengkapnya, lihat Benchmark [CIS untuk CIS Foun AWS Audit Manager d ations Benchmark v1.4.0](#).

2 Maret 2022

[Kerangka kerja baru yang didukung: CIS Controls v8 IG1](#)

Kerangka kerja bawaan baru sekarang tersedia di AWS Audit Manager. Untuk informasi selengkapnya, lihat [CIS Controls v8 IG1](#).

2 Maret 2022

[AWS Audit Manager dasbor](#)

Anda sekarang dapat menggunakan dasbor Audit Manager untuk memantau penilaian aktif Anda dan dengan cepat mengidentifikasi bukti yang tidak sesuai. Untuk informasi selengkapnya, lihat [Menggunakan dasbor Audit Manager](#).

18 November 2021

Berbagi kerangka kerja khusus	Anda sekarang dapat membagikan kerangka Audit Manager kustom Anda dengan yang lain Akun AWS, atau mereplikasinya ke yang Wilayah AWS lain di akun Anda sendiri. Untuk informasi selengkapnya, lihat Berbagi kerangka kerja khusus .	Oktober 22, 2021
Contoh AWS Audit Manager kontrol baru	Anda sekarang dapat meninjau contoh kontrol dan mempelajari bagaimana Audit Manager membantu AWS menyesuaikan lingkungan Anda dengan persyaratan mereka. Untuk informasi selengkapnya, lihat Contoh AWS Audit Manager kontrol .	September 21, 2021
Kerangka kerja baru yang didukung: Gramm-Leach-Bliley Act (GLBA)	Kerangka kerja bawaan baru sekarang tersedia di AWS Audit Manager. Untuk informasi lebih lanjut, lihat Undang Gram-Leach-Bliley dan Undang (GLBA) .	2 September 2021
Bab pemecahan masalah baru	Bab pemecahan masalah baru sekarang tersedia. Untuk informasi selengkapnya, lihat Pemecahan Masalah di AWS Audit Manager .	23 Agustus 2021

Bab delegasi baru dan tutorial	Kami memperluas dokumentasi delegasi kami ke babak baru. Untuk informasi lebih lanjut, lihat Delegasi di AWS Audit Manager . Kami juga menambahkan tutorial baru yang ditujukan untuk delegasi yang meninjau kumpulan kontrol untuk pertama kalinya di AWS Audit Manager. Untuk informasi selengkapnya, lihat Tutorial untuk Delegasi: Meninjau kumpulan kontrol .	25 Juni 2021
Kerangka kerja baru yang didukung: NIST SP 800-171 Rev. 2	Kerangka kerja bawaan baru sekarang tersedia di AWS Audit Manager. Untuk informasi lebih lanjut, lihat NIST SP 800-171 Rev. 2 .	17 Juni 2021
Laporan penilaian yang ditingkatkan	Kami melakukan perbaikan pada format dan isi laporan AWS Audit Manager penilaian. Untuk informasi selengkapnya tentang cara menavigasi dan memahami laporan penilaian baru, lihat Laporan penilaian .	8 Juni 2021
Halaman kebijakan AWS terkelola baru	AWS Audit Manager telah mulai melacak perubahan untuk kebijakan yang dikelola. Untuk informasi selengkapnya, lihat Kebijakan terkelola AWS untuk AWS Audit Manager .	6 Mei 2021

Kerangka kerja baru yang didukung: NIST Cybersecurity Framework versi 1.1	Kerangka kerja bawaan baru sekarang tersedia di AWS Audit Manager. Untuk informasi selengkapnya, lihat Kerangka Kerja Keamanan Siber NIST versi 1.1 .	5 Mei 2021
Kerangka kerja baru yang didukung: AWS Well-Architected	Kerangka kerja bawaan baru sekarang tersedia di AWS Audit Manager. Untuk informasi selengkapnya, lihat AWS Well-Architected .	5 Mei 2021
Kerangka kerja baru yang didukung: AWS Praktik Terbaik Keamanan Dasar	Kerangka kerja bawaan baru sekarang tersedia di AWS Audit Manager. Untuk informasi selengkapnya, lihat AWS Praktik Terbaik Keamanan Dasar .	5 Mei 2021
Kerangka kerja baru yang didukung: GxP EU Annex 11	Kerangka kerja bawaan baru sekarang tersedia di AWS Audit Manager. Untuk informasi lebih lanjut, lihat GxP EU Annex 11 .	28 April 2021
Kerangka kerja baru yang didukung: NIST 800-53 (Rev. 5) Low-Moderate-High	Kerangka kerja bawaan baru sekarang tersedia di AWS Audit Manager. Untuk informasi lebih lanjut, lihat NIST 800-53 (Rev. 5). Low-Moderate-High	25 Maret 2021

[Kerangka kerja baru yang didukung: CIS Benchmark untuk CIS Foun AWS Audit Manager dations Benchmark v1.3](#)

Dua kerangka kerja prebuilt baru sekarang tersedia di AWS Audit Manager: CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0, Level 1, dan CIS Benchmark untuk CIS AWS Audit Manager Foundations Benchmark v1.3.0, Level 1 dan 2. Untuk informasi selengkapnya, lihat Benchmark [CIS untuk CIS Foun AWS Audit Manager dations Benchmark v1.3.0](#).

22 Maret 2021

[Rilis awal](#)

Rilis awal Panduan AWS Audit Manager Pengguna dan Referensi API.

8 Desember 2020