
AWS Audit Manager

User Guide



AWS Audit Manager: User Guide

Copyright © 2023 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

What is AWS Audit Manager?	1
Features of AWS Audit Manager	1
Pricing for AWS Audit Manager	2
Are you a first-time user of Audit Manager?	2
More AWS Audit Manager resources	2
Concepts and terminology	2
A	2
C	4
D	6
E	8
F	9
R	10
S	11
Evidence collection	11
Evidence collection frequency	12
Examples of controls	13
Automated controls (Security Hub)	13
Automated controls (AWS Config)	14
Automated controls (API calls)	16
Automated controls (CloudTrail)	17
Manual controls	18
Controls with mixed data sources	20
AWS service integrations	21
Third-party GRC integrations	22
Understanding third-party integrations	23
Supported third-party GRC products	23
Using Audit Manager with an AWS SDK	24
Setting up	26
Prerequisites	26
Sign up for an AWS account	26
Create an administrative user	26
Add the required permissions	27
Enable Audit Manager	28
Recommendations	31
Recommended features	31
Recommended integrations	31
What do I do next?	35
Get started	35
Update your settings	35
Getting started	36
Audit Manager tutorials	36
Tutorial for Audit Owners: Creating an assessment	36
Step 1: Specify assessment details	37
Step 2: Specify accounts in scope	37
Step 3: Specify services in scope	38
Step 4: Specify audit owners	38
Step 5: Review and create	39
Where do I go from here?	39
Tutorial for Delegates: Reviewing a control set	39
Step 1: Access your notifications	40
Step 2: Review control set and evidence	40
Step 3: Upload manual evidence	41
Step 4: Add a comment	42
Step 5: Update control status	42

Step 6. Submit the reviewed control set back to the audit owner	42
Where do I go from here?	43
Using the dashboard	44
Dashboard concepts and terminology	44
Dashboard elements	46
Assessment filter	46
Daily snapshot	47
Controls with non-compliant evidence grouped by control domain	47
What do I do next?	49
Troubleshooting	49
Assessments	50
Creating an assessment	50
Step 1: Specify assessment details	51
Step 2: Specify accounts in scope	51
Step 3: Specify services in scope	52
Step 4: Specify audit owners	53
Step 5: Review and create	53
What can I do next?	53
Accessing an assessment	54
Editing an assessment	54
Step 1: Edit assessment details	55
Step 2: Edit accounts in scope	55
Step 3: Edit services in scope	55
Step 4: Edit audit owners	56
Step 5: Review and save	56
Reviewing an assessment	56
Assessment details	57
Controls tab	58
Assessment report selection tab	58
AWS accounts tab	59
AWS services tab	59
Audit owners tab	59
Tags tab	60
Changelog tab	60
Reviewing assessment controls	60
Control detail	61
Control status	61
Evidence folders tab	61
Data source tab	62
Comments tab	62
Changelog tab	63
Reviewing evidence	63
Reviewing evidence folders	64
Reviewing individual evidence	65
Adding manual evidence	67
How to add manual evidence	67
Supported file formats	73
Generating an assessment report	73
Adding evidence	74
Removing evidence	74
Generating a report	75
What can I do next?	75
Changing an assessment status	76
Deleting an assessment	77
Delegations	79
For audit owners	79
Delegating a control set	79

Accessing delegations	80
Deleting delegations	81
For delegates	82
Viewing notifications	82
Reviewing controls and evidence	83
Adding comments	83
Marking a control as reviewed	84
Submitting a control set to the audit owner	84
Assessment reports	85
Folder structure	85
How to navigate a report	85
Report sections	86
Cover page	86
Overview page	86
Table of contents page	87
Control page	87
Evidence summary page	88
Evidence detail page	89
Report integrity check	89
Troubleshooting	89
Evidence finder	90
Understanding how evidence finder works with CloudTrail Lake	90
Enabling evidence finder	91
Troubleshooting evidence finder	91
Searching for evidence	91
Performing a search query	91
Stopping a search query	92
Editing search filters	93
Viewing results in evidence finder	93
Viewing the grouped results	94
Viewing the search results	94
Filter and grouping options	99
Filter reference	99
Grouping reference	102
Example use cases	102
Use case 1: Find non-compliant evidence and organize delegations	102
Use case 2: Identify compliant evidence	103
Use case 3: Perform a quick preview of evidence resources	104
Download center	105
Browsing the download center	105
Downloading a file	106
Deleting a file	106
Framework library	107
Accessing a framework	107
Viewing framework details	108
Creating a custom framework	110
Create new	111
Customize existing	112
Editing a custom framework	114
Step 1: Specify framework details	114
Step 2: Edit controls	114
Step 3. Review and update	115
Deleting a custom framework	115
Sharing a custom framework	116
Sharing concepts and terminology	117
Sending a share request	120
Responding to a share request	124

Deleting a share request	127
Supported frameworks	127
ACSC Essential Eight	128
ACSC ISM	129
AWS Audit Manager Sample Framework	131
AWS Control Tower Guardrails	132
AWS generative AI best practices for Amazon Bedrock	133
AWS License Manager	138
AWS Foundational Security Best Practices	140
AWS Operational Best Practices	141
AWS Well-Architected	142
CCCS Medium Cloud Control Profile	144
CIS AWS Foundations Benchmark v.1.2	145
CIS AWS Foundations Benchmark v.1.3	151
CIS AWS Foundations Benchmark v.1.4	154
CIS Controls v7.1 IG1	156
CIS Controls v8 IG1	158
FedRAMP Moderate Baseline	160
General Data Protection Regulation (GDPR)	162
Gramm-Leach-Bliley Act	180
GxP 21 CFR part 11	181
GxP EU Annex 11	183
HIPAA Security Rule 2003	185
HIPAA Final Omnibus Security Rule 2013	187
ISO/IEC 27001:2013	189
NIST 800-53 (Rev. 5)	190
NIST CSF v1.1	192
NIST SP 800-171 (Rev. 2)	194
PCI DSS v3.2.1	196
SOC 2	197
Control library	200
Accessing a control	200
Viewing control details	201
Creating a custom control	203
Create new	204
Customize existing	206
Editing a custom control	208
Step 1: Edit control details	209
Step 2: Edit data sources	209
Step 3: Edit action plan	210
Step 4: Review and update	210
Deleting a custom control	210
Changing evidence collection frequency	211
Configuration snapshots from API calls	212
Compliance checks from AWS Config	212
Compliance checks from Security Hub	213
User activity logs from AWS CloudTrail	213
Control data sources	213
Automated data sources	214
AWS Config	215
AWS Security Hub	224
AWS API calls	247
AWS CloudTrail	249
Settings	251
General settings	251
Permissions	251
Data encryption	252

Delegated administrator (optional)	253
AWS Config (optional)	257
Security Hub (optional)	258
Disable AWS Audit Manager	258
Assessment settings	259
Default audit owners (optional)	260
Assessment report destination (optional)	260
Notifications (optional)	262
Evidence finder settings	263
Evidence finder (optional)	263
Export destination (optional)	267
Notifications	270
Prerequisites	270
Configuring notifications in AWS Audit Manager	270
Troubleshooting	271
Troubleshooting	272
Assessments and evidence collection	272
I created an assessment but I can't see any evidence yet	273
My assessment isn't collecting compliance check evidence from AWS Security Hub	273
My assessment isn't collecting compliance check evidence from AWS Config	274
My assessment isn't collecting user activity evidence from AWS CloudTrail	276
My assessment isn't collecting configuration data evidence for an AWS API call	276
My assessment isn't collecting evidence from another AWS service	276
My evidence is generated at different intervals, and I'm not sure how often it's being collected ..	277
What happens if I remove an in-scope account from my organization?	277
I can't edit the services in scope for my assessment	278
What's the difference between a service in scope and a data source type?	278
My assessment creation failed	279
I disabled and then re-enabled Audit Manager, and now my pre-existing assessments are no longer collecting evidence	279
Assessment reports	279
My assessment report failed to generate	279
I followed the checklist above, and my assessment report still failed to generate	280
I get an <i>access denied</i> error when I try to generate a report	281
I'm unable to unzip the assessment report	281
When I choose an evidence name in a report, I'm not redirected to the evidence details	281
My assessment report generation is stuck in <i>In progress</i> status, and I'm not sure how this impacts my billing	282
See also	282
Controls and control sets	282
I can't see any controls or control sets in my assessment	283
I can't upload manual evidence to a control	283
I need to use multiple AWS Config rules as a data source for a single control	283
The custom rule option is unavailable for my data source	283
The dropdown list of custom rules is empty	283
I can't see the custom rule that I want to use	284
I can't see the managed rule that I want to use	285
I want to share a custom framework, but it has controls that use custom AWS Config rules as a data source	287
What happens when a custom rule is updated in AWS Config?	287
Dashboard	288
There isn't any data on my dashboard	288
The CSV download option isn't available	288
I don't see the downloaded file when trying to download a CSV file	289
A specific control or control domain is missing from the dashboard	289
The daily snapshot shows varying amounts of evidence each day. Is this normal?	289
Delegated administrators and AWS Organizations	289

I can't set up Audit Manager with my delegated administrator account	290
When I create an assessment, I can't see the accounts from my organization under <i>Accounts in scope</i>	290
I get an <i>access denied</i> error when I try to generate an assessment report using my delegated administrator account	290
What happens in Audit Manager if I unlink a member account from my organization?	291
What happens if I relink a member account to my organization?	291
What happens if I migrate a member account from one organization to another?	291
Evidence finder	292
I can't enable evidence finder	292
I enabled evidence finder, but I don't see past evidence in my search results	293
I can't disable evidence finder	293
My search query fails	293
I can't generate multiple assessment reports from my search results	295
I can't include specific evidence from my search results	295
Not all of my evidence finder results are included in the assessment report	295
I want to generate an assessment report from my search results, but my query statement is failing	296
More resources	298
My CSV export failed	298
I can't export specific evidence from my search results	299
I can't export multiple CSV files at once	299
Framework sharing	300
My sent share request status displays as <i>Failed</i>	300
My share request has a blue dot next to it. What does this mean?	300
My shared framework has controls that use custom AWS Config rules as a data source. Can the recipient collect evidence for these controls?	302
I updated a custom rule that's used in a shared framework. Do I need to take any action?	303
Notifications	303
I specified an Amazon SNS topic in Audit Manager, but I'm not receiving any notifications	304
I specified a FIFO topic, but I'm not receiving notifications in the expected order	304
Permissions and access	304
I followed the Audit Manager setup procedure, but I don't have enough IAM privileges	304
I specified someone as an audit owner, but they still don't have full access to the assessment.	
Why is this?	305
I can't perform an action in Audit Manager	305
I want to allow people outside of my AWS account to access my Audit Manager resources	305
See also	282
Quotas	307
Default Audit Manager quotas	307
Managing your quotas	308
Security	309
Data protection	309
Deletion of Audit Manager data	310
Encryption at rest	311
Encryption in transit	311
Key management	311
Identity and access management	312
Audience	312
Authenticating with identities	313
Managing access using policies	315
How AWS Audit Manager works with IAM	316
Identity-based policy examples	323
Cross-service confused deputy prevention	336
AWS managed policies	337
Troubleshooting	350
Using service-linked roles	351

Compliance validation	358
Resilience	359
Infrastructure security	359
VPC endpoints (AWS PrivateLink)	359
Considerations for AWS Audit Manager VPC endpoints	360
Creating an interface VPC endpoint for AWS Audit Manager	360
Creating a VPC endpoint policy for AWS Audit Manager	360
Logging and monitoring	361
Monitoring with Amazon EventBridge	361
CloudTrail logs	364
Configuration and vulnerability	366
Tagging resources	367
Supported resources	367
Tag restrictions	367
Managing tags in Audit Manager	367
AWS CloudFormation resources	369
Audit Manager and AWS CloudFormation templates	369
Learn more about AWS CloudFormation	369
Document history	370
AWS Glossary	376

What is AWS Audit Manager?

Welcome to the AWS Audit Manager User Guide.

AWS Audit Manager helps you continually audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards. Audit Manager automates evidence collection so you can more easily assess whether your policies, procedures, and activities—also known as *controls*—are operating effectively. When it's time for an audit, Audit Manager helps you manage stakeholder reviews of your controls. This means that you can build audit-ready reports with much less manual effort.

Audit Manager provides prebuilt frameworks that structure and automate assessments for a given compliance standard or regulation. Frameworks include a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped according to the requirements of the specified compliance standard or regulation. You can also customize frameworks and controls to support internal audits according to your specific requirements.

You can create an assessment from any framework. When you create an assessment, Audit Manager automatically runs resource assessments. These assessments collect data for both the AWS account and services that you define as in scope for your audit. The data that's collected is automatically transformed into audit-friendly evidence. Then, it's attached to the relevant controls to help you demonstrate compliance in security, change management, business continuity, and software licensing. This evidence collection process is ongoing, and starts when you create your assessment. After you complete an audit and you no longer need Audit Manager to collect evidence, you can stop evidence collection. To do this, change the status of your assessment to *inactive*.

Features of Audit Manager

With AWS Audit Manager, you can do the following tasks:

- **Get started quickly** — [Create your first assessment](#) by selecting from a gallery of prebuilt frameworks that support a range of compliance standards and regulations. Then, initiate automatic evidence collection to audit your AWS service usage.
- **Upload and manage evidence from hybrid or multicloud environments** — In addition to the evidence that Audit Manager collects from your AWS environment, you can also [upload](#) and centrally manage evidence from your on-premises or multicloud environment.
- **Support common compliance standards and regulations** — Choose one of the [AWS Audit Manager standard frameworks](#). These frameworks provide prebuilt control mappings for common compliance standards and regulations. These include the CIS Foundation Benchmark, PCI DSS, GDPR, HIPAA, SOC2, GxP, and AWS operational best practices.
- **Monitor your active assessments** — Use the Audit Manager [dashboard](#) to view analytics data for your active assessments, and quickly identify non-compliant evidence that needs to be remediated.
- **Search for evidence** — Use the [evidence finder](#) feature to quickly find evidence that's relevant to your search query. You can generate an assessment report from your search results, or export your search results in CSV format.
- **Create custom controls** — [Create your own control from scratch](#) or [customize an existing control to meet your needs](#). You can also use the custom controls feature to create risk assessment questions and store the responses to those questions as manual evidence.
- **Customize frameworks** — [Create your own frameworks](#) with standard or custom controls based on your specific requirements for internal audits.
- **Share custom frameworks** — [Share your custom Audit Manager frameworks](#) with another AWS account, or replicate them into another AWS Region under your own account.

- **Support cross-team collaboration** — [Delegate control sets](#) to subject matter experts who can review related evidence, add comments, and update the status of each control.
- **Create reports for auditors** — [Generate assessment reports](#) that summarize the relevant evidence that's collected for your audit and link to folders that contain the detailed evidence.
- **Ensure evidence integrity** — [Store evidence](#) in a secure location, where it remains unaltered.

Note

AWS Audit Manager assists in collecting evidence that's relevant for verifying compliance with specific compliance standards and regulations. However, it doesn't assess your compliance itself. The evidence that's collected through AWS Audit Manager therefore might not include all the information about your AWS usage that's needed for audits. AWS Audit Manager isn't a substitute for legal counsel or compliance experts.

Pricing for Audit Manager

For more information about pricing, see [AWS Audit Manager Pricing](#).

Are you a first-time user of Audit Manager?

If you're a first-time user of Audit Manager, we recommend that you start with the following pages:

1. [AWS Audit Manager concepts and terminology](#) – Learn about the key concepts and terms used in Audit Manager, such as assessments, frameworks, and controls.
2. [How AWS Audit Manager collects evidence](#) – Learn about how Audit Manager gathers evidence for a resource assessment.
3. [Setting up](#) – Learn about the setup requirements for Audit Manager.
4. [Getting Started](#) – Follow a tutorial to create your first Audit Manager assessment.
5. [AWS Audit Manager API Reference](#) – Familiarize yourself with the Audit Manager API actions and data types.

More Audit Manager resources

Explore the following resources to learn more about Audit Manager.

- [Collect Evidence and Manage Audit Data Using AWS Audit Manager](#)
- [Manually configure a custom Audit Manager assessment](#) from [AWS Workshops](#)
- [Integrate across the Three Lines Model \(Part 2\): Transform AWS Config conformance packs into AWS Audit Manager assessments](#) from the [AWS Management & Governance Blog](#)

AWS Audit Manager concepts and terminology

To help you get started, this page defines terms and explains some of the key concepts of AWS Audit Manager.

A

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Assessment

You can use an Audit Manager assessment to automatically collect evidence that's relevant for an audit.

An assessment is based on a framework, which is a grouping of controls that are related to your audit. Depending on your business requirements, you can create an assessment from a standard framework or a custom framework. Standard frameworks contain prebuilt control sets that support a specific compliance standard or regulation. In contrast, custom frameworks contain controls that you can customize and group according to your internal audit requirements. Using a framework as a starting point, you can create an assessment that specifies the AWS accounts and services that you want to include in the scope of your audit.

When you create an assessment, Audit Manager automatically starts to assess resources in your AWS accounts and services based on the controls that are defined in the framework. Next, it collects the relevant evidence and converts it into an auditor-friendly format. After doing this, it then attaches the evidence to the controls in your assessment. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. This assessment report helps you to demonstrate that your controls are working as intended.

Evidence collection is an ongoing process that starts when you create your assessment. You can stop evidence collection by changing the assessment status to *inactive*. Alternatively, you can stop evidence collection at the control level. You can do this by changing the status of a specific control within your assessment to *inactive*.

For instructions on how to create and manage assessments, see [Assessments in AWS Audit Manager \(p. 50\)](#).

Assessment report

An assessment report is a finalized document that's generated from an Audit Manager assessment. These reports summarize the relevant evidence that's collected for your audit. They link to the relevant evidence folders. The folders are named and organized according to the controls that are specified in your assessment. For each assessment, you can review the evidence that Audit Manager collects, and decide which evidence you want to include in the assessment report.

To learn more about assessment reports, see [Assessment reports \(p. 85\)](#). To learn how to generate an assessment report, see [Generating an assessment report \(p. 73\)](#).

Assessment report destination

An assessment report destination is the default S3 bucket where Audit Manager saves your assessment reports. To learn more, see [Assessment report destination \(optional\) \(p. 260\)](#).

Audit

An audit is an independent examination of the assets, operations, or business integrity of your organization. An information technology (IT) audit specifically examines the controls within the information systems of your organization. The goal of an IT audit is to determine if information systems safeguard assets, operate effectively, and maintain data integrity. All of these are important to meeting the regulatory requirements that are mandated by a compliance standard or regulation.

Audit owner

The term *audit owner* has two different meanings depending on the context.

In the context of Audit Manager, an audit owner is a user or role that manages an assessment and its related resources. The responsibilities of this Audit Manager persona include creating assessments, reviewing evidence, and generating assessment reports. Audit Manager is a collaborative service, and audit owners benefit when other stakeholders participate in their assessments. For example, you can add other audit owners to your assessment to share management tasks. Or, if you're an audit owner

and you need help interpreting the evidence that was collected for a control, you can [delegate that control set](#) to a stakeholder who has subject matter expertise in that area. Such a person is known as a *delegate* persona.

In business terms, an audit owner is someone who coordinates and oversees the audit readiness efforts of their company, and presents evidence to an auditor. Typically, this is a governance, risk, and compliance (GRC) professional, such as a Compliance Officer or a GDPR Data Protection Officer. GRC professionals have the expertise and authority to manage audit preparation. More specifically, they understand compliance requirements, and can analyze, interpret, and prepare reporting data. However, other business roles can also assume the Audit Manager persona of an audit owner—not only GRC professionals take on this role. For example, you might choose to have your Audit Manager assessments set up and managed by a technical expert from one of the following teams:

- SecOps
- IT/DevOps
- Security Operations Center/Incident Response
- Similar teams that own, develop, remediate, and deploy cloud assets, and understand the cloud infrastructure of your organization

Who you choose to assign as an audit owner in your Audit Manager assessment depends greatly on your organization. It also depends on how you structure your security operations and the specifics of the audit. In Audit Manager, the same individual can assume the audit owner persona in one assessment, and the delegate persona in another.

No matter how you choose to use Audit Manager, you can manage the separation of duties across your organization using the audit owner/delegate persona and granting specific IAM policies to each user. Through this two-step approach, Audit Manager ensures that you have full control over all of the specifics of an individual assessment. For more information, see [Recommended policies for user personas in AWS Audit Manager](#).

C

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Changelog

For each control in an assessment, Audit Manager captures changelogs to track user activity for that control. You can then review an audit trail of activities that are related to a specific control. For more information about which user activities are captured in changelogs, see [Changelog tab \(p. 63\)](#).

Cloud compliance

Cloud compliance is the general principle that cloud-delivered systems must be compliant with the standards that are faced by cloud customers.

Compliance regulation

A compliance regulation is a law, rule, or other order that's prescribed by an authority, typically to regulate conduct. One example is GDPR.

Compliance standard

A compliance standard is a structured set of guidelines that detail the processes of an organization for maintaining accordance with established regulations, specifications, or legislation. Examples include PCI DSS and HIPAA.

Control

A control is a safeguard or countermeasure that's prescribed for an information system or an organization. Controls are designed to protect the confidentiality, integrity, and availability of

your information, and to meet a set of defined security requirements. They provide an assurance that your resources are operating as intended, your data is reliable, and your organization is in compliance with applicable laws and regulations.

In Audit Manager, a control can also represent a question in a vendor risk assessment questionnaire. In this case, a control is a specific question that asks information about an organization's security and compliance posture.

Controls collect evidence continually when they're active in your Audit Manager assessments. You can also manually add evidence to any control. Each piece of evidence becomes a record that helps you to demonstrate compliance with the control's requirements.

There are two types of control in Audit Manager:

- **Standard controls** — These are prebuilt controls that are associated with a specific framework in Audit Manager. Use standard controls to assist you with audit preparation for various compliance standards and regulations.
- **Custom controls** — These are customized controls that you define as an Audit Manager user. Use custom controls to help you meet specific compliance requirements for internal audits or vendor risk assessments.

For more information, see [Examples of AWS Audit Manager controls](#). For instructions on how to create and manage controls, see [Control library \(p. 200\)](#).

Control domains

You can think of a control domain as a general category of controls that isn't specific to any one framework. Control domain groupings are one of the most powerful features of the [Audit Manager dashboard](#). Audit Manager highlights the controls in your assessments that have non-compliant evidence, and groups them by control domain. This enables you to focus your remediation efforts on specific subject domains as you prepare for an audit.

Note

A control domain is different to a *control set*. A control set is a framework-specific grouping of controls that's typically defined by a regulatory body. For example, the PCI DSS framework has a control set named *Requirement 8: Identify and authenticate access to system components*. This control set falls under the control domain of *Identity and access management*.

Audit Manager categorizes controls under the following control domains.

Control domain name	Description of what these controls govern
Business continuity and contingency planning	How you establish processes that protect critical business operations from the effects of major system and network disruptions.
Change management	How you test, approve, implement, and document changes to your cloud infrastructure.
Data security and privacy	How you secure the privacy, availability, and integrity of your data.
Development and configuration management	How you maintain your cloud infrastructure in a desired and consistent state.
Governance and oversight	How you align your use of cloud computing with your legal, regulatory, and ethical obligations.

Control domain name	Description of what these controls govern
Identity and access management	How you ensure that the right users have the appropriate access to your technology resources.
Incident management	How you establish responsibilities and procedures that ensure a quick and effective response to security incidents.
Logging and monitoring	How you review user activity for indications that unauthorized activity was attempted or performed.
Network management	How you administer and operate your data network using a network management system.
Personnel management	How you assess and manage personnel security risks at an organizational level.
Physical security	How you detect and prevent physical security issues in your facilities.
Risk management	How you evaluate potential risks and losses, and how you reduce or eliminate such threats.
Supply chain management	How you identify, assess, and mitigate the risks that are associated with IT products, vendors, and supply chains.
User device management	How you reduce the risk that your employees' IT hardware is lost, damaged, or compromised.
Vulnerability management	How you define, assess, and remediate all known vulnerabilities for assets within your cloud infrastructure.

D

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Data source

Audit Manager uses a *data source* to collect evidence for a control. The following terminology describes what a data source is and how it works.

- A **Data source type** defines where Audit Manager collects evidence for a control. If you upload your own evidence, the data source type is *Manual*. If Audit Manager collects the evidence on your behalf, the data source type is one of the following: *AWS Security Hub*, *AWS Config*, *AWS CloudTrail*, or *AWS API calls*. The Audit Manager API refers to a data source type as a [sourceType](#) (singular) or [controlSources](#) (plural).
- A **Mapping** is a specific keyword that relates to a data source type. For example, this might be a CloudTrail event name or an AWS Config name. The Audit Manager API refers to this as a [sourceKeyword](#) (singular) or [controlMappingSources](#) (plural).
- A **Data source name** is a name that's given to a data source. In other words, a data source name labels the combination of a data source type and mapping. For standard controls, Audit Manager provides a default data source name (such as *Data source 1* and *Data source 2*). For custom controls, you can provide your own data source name. This might help you to distinguish between multiple mappings that fall under the same data source type. The Audit Manager API refers to a data source name as a [sourceName](#).

A single control can have multiple data source types and multiple mappings. For example, one control might collect evidence from a mixture of data source types (such as AWS Config and Security

Hub). Another control might have AWS Config as its only data source type, with multiple AWS Config rules as mappings.

The following table lists the automated data source types and shows examples of some corresponding mappings.

Data source type	Description	Mapping example
AWS Security Hub	Use this data source type to capture a snapshot of your resource security posture. Audit Manager uses the name of a Security Hub control as the mapping keyword, and reports the result of that security check directly from Security Hub.	1.1 – Avoid the use of the "root" account
AWS Config	Use this data source type to capture a snapshot of your resource security posture. Audit Manager uses the name of an AWS Config rule as the mapping keyword, and reports the result of that rule check directly from AWS Config.	EC2_INSTANCE_MANAGED_BY_SSM
AWS CloudTrail	Use this data source type to track a specific user activity that's needed in your audit. Audit Manager uses the name of a CloudTrail event as the mapping keyword, and collects the related user activity from your CloudTrail logs.	CreateAccessKey
AWS API calls	Use this data source type to take a snapshot of your resource configuration through an API call to a specific AWS service. Audit Manager uses the name of API call as the mapping keyword, and collects the API response.	ec2_DescribeSecurityGroups

The following image shows examples of different data sources as seen in the Audit Manager console.

Details	Data sources	Tags																				
Data sources (4)																						
<table border="1"> <thead> <tr> <th>Data source name</th> <th>Data source type</th> <th>Mapping</th> <th>Frequency</th> </tr> </thead> <tbody> <tr> <td>Data source 1</td> <td>AWS API calls</td> <td>iam_ListRoles</td> <td>Daily</td> </tr> <tr> <td>Data source 2</td> <td>AWS API calls</td> <td>iam_ListGroups</td> <td>Daily</td> </tr> <tr> <td>Data source 3</td> <td>AWS API calls</td> <td>iam_ListUsers</td> <td>Daily</td> </tr> <tr> <td>Data source 4</td> <td>AWS API calls</td> <td>iam_ListPolicies</td> <td>Daily</td> </tr> </tbody> </table>			Data source name	Data source type	Mapping	Frequency	Data source 1	AWS API calls	iam_ListRoles	Daily	Data source 2	AWS API calls	iam_ListGroups	Daily	Data source 3	AWS API calls	iam_ListUsers	Daily	Data source 4	AWS API calls	iam_ListPolicies	Daily
Data source name	Data source type	Mapping	Frequency																			
Data source 1	AWS API calls	iam_ListRoles	Daily																			
Data source 2	AWS API calls	iam_ListGroups	Daily																			
Data source 3	AWS API calls	iam_ListUsers	Daily																			
Data source 4	AWS API calls	iam_ListPolicies	Daily																			

Note

Although some data source types are AWS services, a data source type is different to a *service in scope*. For more information, see [What's the difference between a service in scope and a data source type?](#) in the *Troubleshooting* section of this guide.

Delegate

A delegate is an AWS Audit Manager user with limited permissions. Delegates typically have specialized business or technical expertise. For example, these expertise might be in data retention policies, training plans, network infrastructure, or identity management. Delegates help audit owners review collected evidence for controls that are in their area of expertise. Delegates can review control sets and their related evidence, add comments, upload additional evidence, and update the status of each of the controls that you assign to them for review.

Audit owners assign specific control sets to delegates, not entire assessments. As a result, delegates have limited access to assessments. For instructions on how to delegate a control set, see [Delegations in AWS Audit Manager \(p. 79\)](#).

E

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Evidence

Evidence is a record that contains the information that's needed to demonstrate compliance with a control's requirements. Examples of evidence include a change activity invoked by a user, and a system configuration snapshot.

There are two main types of evidence in Audit Manager: *automated evidence* and *manual evidence*.

- **Automated evidence** — This is the evidence that Audit Manager collects automatically. This includes the following three categories of automated evidence:
 - **Compliance check** — The result of a compliance check is captured from AWS Security Hub, AWS Config, or both. Examples of compliance checks include a security check result from Security Hub for a PCI DSS control, and an AWS Config rule evaluation for a HIPAA control. For more information, see [AWS Config Rules supported by AWS Audit Manager](#) and [AWS Security Hub controls supported by AWS Audit Manager](#).
 - **User activity** — User activity that changes a resource configuration is captured from CloudTrail logs as that activity occurs. Examples of user activities include a route table update, an Amazon RDS instance backup setting change, and an S3 bucket encryption policy change. For more information, see [AWS CloudTrail event names supported by AWS Audit Manager](#).
 - **Configuration data** — A snapshot of the resource configuration is captured directly from an AWS service on a daily, weekly, or monthly basis. Examples of configuration snapshots include a list of routes for a VPC route table, an Amazon RDS instance backup setting, and an S3 bucket encryption policy. For more information, see [API calls supported by AWS Audit Manager](#).
- **Manual evidence** — This is the evidence that you add to Audit Manager yourself. There are three ways to add your own evidence:
 - Import a file from Amazon S3
 - Upload a file from your browser
 - Enter a text response to a risk assessment question

For more information, see [Adding manual evidence in AWS Audit Manager \(p. 67\)](#).

Automated evidence collection starts when you create an assessment. This is an ongoing process, and Audit Manager collects evidence at different frequencies depending on the evidence type and the underlying data source. For more information about evidence collection, see [How AWS Audit](#)

[Manager collects evidence \(p. 11\)](#). For instructions on how to review evidence in an assessment, see [Reviewing the evidence in an assessment \(p. 63\)](#).

Evidence collection method

There are two ways that a control can collect evidence.

- **Automated controls** automatically collect evidence from AWS data sources. This automated evidence can help you to demonstrate full or partial compliance with the control.
- **Manual controls** require you to [upload your own evidence](#) to demonstrate compliance with the control.

Note

You can attach manual evidence to any automated control. In many cases, a combination of automated and manual evidence is needed to demonstrate full compliance with a control. Although Audit Manager can provide automated evidence that's helpful and relevant, some automated evidence might only demonstrate partial compliance. In this case, you can supplement the automated evidence that Audit Manager provides with your own evidence. For example:

- The [AWS generative AI best practices framework](#) contains a control called Error analysis. This control requires you to identify when inaccuracies are detected in your model usage. It also requires you to conduct a thorough error analysis to understand the root causes and take corrective action.
- To support this control, Audit Manager collects automated evidence that shows if CloudWatch alarms are enabled for the AWS account where your assessment is running. You can use this evidence to demonstrate partial compliance with the control by proving that your alarms and checks are configured correctly.
- To demonstrate full compliance, you can supplement the automated evidence with manual evidence. For example, you can upload a policy or a procedure that shows your error analysis process, your thresholds for escalations and reporting, and the results of your root cause analysis. You can use this manual evidence to demonstrate that established policies are in place, and that corrective action was taken when prompted.

For a more detailed example, see [Controls with mixed data sources](#).

Export destination

An export destination is the default S3 bucket where Audit Manager saves the files that you export from evidence finder. To learn more, see [Export destination \(optional\) \(p. 267\)](#).

F

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Framework

An Audit Manager framework is a file that's used to structure and automate assessments for a specific standard or risk governance principle. These frameworks help map your AWS resources to the requirements in a control. They include a collection of prebuilt or customer defined controls. The collection has descriptions and testing procedures for each control. These controls are organized and grouped based on the requirements of a specified compliance standard or regulation. Examples include PCI DSS, and GDPR.

There are two types of framework in Audit Manager:

- **Standard frameworks** — Prebuilt frameworks that are based on AWS best practices for various compliance standards and regulations. You can use these frameworks to assist with audit preparation.

- **Custom frameworks** — Customized frameworks that you define as an Audit Manager user. You can use these frameworks to assist with audit preparation according to your specific compliance or risk governance requirements.

For instructions on how to create and manage frameworks, see [Framework library \(p. 107\)](#).

Note

AWS Audit Manager assists in collecting evidence that's relevant for verifying compliance with specific compliance standards and regulations. However, it doesn't assess your compliance itself. The evidence that's collected through AWS Audit Manager therefore might not include all the information about your AWS usage that's needed for audits. AWS Audit Manager isn't a substitute for legal counsel or compliance experts.

Framework sharing

You can use the [custom framework sharing feature](#) of Audit Manager to quickly share your custom frameworks across AWS accounts and Regions. To share a custom framework, you create a *share request*. The recipient of the share request then has 120 days to accept or decline the request. When they accept, Audit Manager replicates the shared custom framework into their framework library. In addition to replicating the custom framework, Audit Manager also replicates any custom control sets and controls that are contained within that framework. These custom controls are added to the recipient's control library. Audit Manager doesn't replicate standard frameworks or controls. This is because these resources are already available by default in each account and Region.

R

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

Resource

A resource is a physical or information asset that's assessed in an audit. Examples of AWS resources include Amazon EC2 instances, Amazon RDS instances, Amazon S3 buckets, and Amazon VPC subnets.

Resource assessment

A resource assessment is the process of assessing an individual resource. This assessment is based on the requirement of a control. While an assessment is active, Audit Manager runs resource assessments for each individual resource in the scope of the assessment. A resource assessment runs the following set of tasks:

1. Collects evidence including resource configurations, event logs, and findings
2. Translates and maps evidence to controls
3. Stores and tracks the lineage of evidence to enable integrity

Resource compliance

Resource compliance refers to the evaluation status of a resource that was assessed when collecting compliance check evidence.

Audit Manager collects [compliance check evidence](#) for controls that use AWS Config and Security Hub as a data source type. Multiple resources might be assessed during this evidence collection. As a result, a single piece of compliance check evidence can include one or more resources.

You can use the **Resource compliance** filter in evidence finder to explore compliance status at the resource level. After your search is complete, you can then preview the resources that matched your search query.

In evidence finder, there are three possible values for resource compliance:

- **Non-compliant** – This refers to resources with compliance check issues. This happens if Security Hub reports a *Fail* result for the resource, or if AWS Config reports a *Non-compliant* result.
- **Compliant** – This refers to resources that don't have compliance check issues. This happens if Security Hub reports a *Pass* result for the resource, or if AWS Config reports a *Compliant* result.
- **Inconclusive** – This refers to resources for which a compliance check isn't available or applicable. This happens if AWS Config or Security Hub is the underlying data source type, but those services aren't enabled. This also happens if the underlying data source type doesn't support compliance checks (such as manual evidence, AWS API calls, or CloudTrail).

S

A|B|[C](#)|[D](#)|[E](#)|[F](#)|G|H|I|J|K|L|M|N|O|P|Q|[R](#)|[S](#)|T|U|V|W|X|Y|Z

Service in scope

This is an AWS service that's included in the scope of your assessment. When you specify a service as being included in the scope of your assessment, Audit Manager assesses that service's resources. Audit Manager can assess a large variety of resources from a service in scope. Some example resources include the following:

- An Amazon EC2 instance
- An S3 bucket
- A user or role
- A DynamoDB table
- A network component such as an Amazon Virtual Private Cloud (VPC), security group, or network access control list (ACL) table

When you use the Audit Manager console to create or update an assessment from a standard framework, the list of AWS services in scope is preselected by default. This list can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the standard framework. If a standard framework that contains only manual controls, no AWS services are in scope for your assessment, and you can't add any services to your assessment.

If you need to edit the list of services in scope for a standard framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

Note

Keep in mind that a service in scope is different to a *data source type*, which can also be an AWS service or something else. For more information, see [What's the difference between a service in scope and a data source type?](#) in the *Troubleshooting* section of this guide.

How AWS Audit Manager collects evidence

Each active assessment in AWS Audit Manager automatically collects evidence from a range of data sources. Every assessment has a defined scope that specifies the AWS services and accounts where Audit Manager collects data from. Each of these defined services and accounts in scope contain multiple resources, and each resource is a system asset inventory that you own. Evidence collection in Audit Manager involves the assessment of each in-scope resource. This is referred to as a *resource assessment*.

The following steps describe how Audit Manager collects evidence for each resource assessment:

1. Assessing a resource from the data source

To start evidence collection, Audit Manager assesses an in-scope resource from a data source. It does this by capturing a configuration snapshot, a related compliance check result, and any user activities. It then runs an analysis to determine which control this data supports. The result of the resource assessment is then saved and converted into evidence. For more information about different evidence types, see [Evidence](#) in the *AWS Audit Manager concepts and terminology* section of this guide.

2. Converting assessment results to evidence

The result of the resource assessment contains both the original data that's captured from that resource, and the metadata that indicates which control the data supports. AWS Audit Manager converts the original data into an auditor-friendly format. The converted data and metadata are then saved as Audit Manager evidence before being attached to a control.

3. Attaching evidence to the related control

Audit Manager reads the evidence metadata. Then, it attaches the saved evidence to a related control within the assessment. The attached evidence becomes visible in Audit Manager. This completes the cycle of a resource assessment.

Note

Depending on the control configurations, the same evidence can, in some cases, be attached to multiple controls from multiple Audit Manager assessments. When the same evidence is attached to multiple controls, Audit Manager meters the resource assessment exactly once. This is because the same evidence is collected exactly only once. However, one control in an Audit Manager assessment can have multiple pieces of evidence from multiple data sources.

Evidence collection frequency

Evidence collection is an ongoing process that starts when you create your assessment. AWS Audit Manager collects evidence from multiple data sources at varying frequencies. As a result, there's no one-size-fits-all answer for how often evidence is collected. The frequency of evidence collection is based on the evidence type and its data source, as described below.

- **Compliance checks** — Audit Manager collects this evidence type from AWS Security Hub and AWS Config.
 - For AWS Security Hub, the frequency of evidence collection follows the schedule of your Security Hub checks. For more information about the schedule of Security Hub checks, see [Schedule for running security checks](#) in the *AWS Security Hub User Guide*. For more information about the Security Hub checks supported by Audit Manager, see [AWS Security Hub controls supported by AWS Audit Manager \(p. 224\)](#).
 - For AWS Config, the frequency of evidence collection follows the triggers that are defined in your AWS Config rules. For more information about the triggers for AWS Config rules, see [Trigger types](#) in the *AWS Config User Guide*. For more information about the AWS Config Rules that are supported by Audit Manager, see [AWS Config Rules supported by AWS Audit Manager \(p. 215\)](#).
- **User activity** — Audit Manager collects this evidence type from AWS CloudTrail in a continual manner. This frequency is continual because user activity can happen at any time of the day. For more information, see [AWS CloudTrail event names supported by AWS Audit Manager \(p. 249\)](#).
- **Configuration data** — Audit Manager collects this evidence type using a describe API call to another AWS service such as Amazon EC2, Amazon S3, or IAM. You can choose which API actions to call. You also set the frequency as daily, weekly, or monthly in Audit Manager. You can specify this frequency when you create or edit a control in the control library. For instructions on how to edit or create a control, see [Control library \(p. 200\)](#). For more information about how Audit Manager uses API calls to create evidence, see [API calls supported by AWS Audit Manager \(p. 247\)](#).

Regardless of the evidence collection frequency for the data source, new evidence is collected automatically for as long as the control and the assessment are active.

Examples of AWS Audit Manager controls

You can review the examples on this page to learn more about how controls work in AWS Audit Manager. These examples describe what a control looks like, how Audit Manager generates evidence for that control, and the next steps that you can take to demonstrate compliance.

Tip

We recommend that you enable AWS Config and AWS Security Hub for an optimal experience in Audit Manager. When you enable these services, they can be used as a data source type for the controls in your Audit Manager assessments. In other words, Audit Manager can use Security Hub findings and AWS Config Rules to generate automated evidence.

- After you [enable AWS Security Hub](#), make sure that you also [enable all security standards](#) and [turn on the consolidated control findings setting](#). This step ensures that Audit Manager can import findings for all supported compliance standards.
- After you [enable AWS Config](#), make sure that you also [enable the relevant AWS Config Rules](#) or [deploy a conformance pack](#) for the compliance standard that's related to your audit. This step ensures that Audit Manager can import findings for all the supported AWS Config Rules that you enabled.

Examples are available for each of the following types of controls:

Topics

- [Automated controls that use AWS Security Hub as a data source type \(p. 13\)](#)
- [Automated controls that use AWS Config as a data source type \(p. 14\)](#)
- [Automated controls that use AWS API calls as a data source type \(p. 16\)](#)
- [Automated controls that use AWS CloudTrail as a data source type \(p. 17\)](#)
- [Manual controls \(p. 18\)](#)
- [Controls with mixed data source types \(automated and manual\) \(p. 20\)](#)

Automated controls that use AWS Security Hub as a data source type

This example shows a control that uses AWS Security Hub as its data source type. This is a standard control taken from the [AWS Foundational Security Best Practices \(FSBP\) framework](#). Audit Manager uses this control to generate evidence that can help to bring your AWS environment in line with FSBP requirements.

Example control details

- **Control name** – IAM policies should not allow full "*" administrative privileges
- **Control set** – This control belongs to the IAM control set. This is a grouping of controls that relate to identity and access management.
- **Data source type** – AWS Security Hub
- **Evidence type** – Compliance check

In the following example, this control is within an Audit Manager assessment that was created from the FSBP framework.

Control sets (27)				Delegate control set	Complete control set review
Q IAM policies should not allow full '*' administrative privileges		X	1 match	< 1 >	②
Controls grouped by control set		Control status	Delegated to	Total evidence	Added to assessment report
○	▼ IAM (8)	② Active	-	0	0
	IAM policies should not allow full '*' administrative privileges	② Under review	-	0	0

The assessment shows the control status. It also shows how much evidence was collected for this control so far and how much of that evidence is included in your assessment report. From here, you can delegate the control set for review or complete the review yourself. Choosing the control name opens a detail page with more information, including the evidence for that control.

What this control does

Audit Manager can use this control to check whether your IAM policies are too broad to meet FSBP requirements. More specifically, it can check whether your customer managed IAM policies have administrator access that includes the following wildcard statement: "Effect": "Allow" with "Action": "*" over "Resource": "*".

How Audit Manager collects evidence for this control

Audit Manager takes the following steps to collect evidence for this control:

1. For each control, Audit Manager assesses your in-scope resources. It does this using the data source that's specified in the control settings. In this example, your IAM policies are the resource, and Security Hub and AWS Config are the data source type. Audit Manager looks for the result of a specific Security Hub check ([\[IAM.1\]](#)), which in turn uses an AWS Config rule to evaluate your IAM policies ([iam-policy-no-statements-with-admin-access](#)).
2. The result of the resource assessment is saved and converted into auditor-friendly evidence. Audit Manager generates *compliance check* evidence for controls that use Security Hub as a data source type. This evidence contains the result of the compliance check reported directly from Security Hub.
3. Audit Manager attaches the saved evidence to the control in your assessment that's named IAM policies should not allow full '*' administrative privileges.

How you can use Audit Manager to demonstrate compliance with this control

After the evidence is attached to the control, you—or a delegate of your choice—can review the evidence to see if any remediation is necessary.

In this example, Audit Manager might display a *Fail* ruling from Security Hub. This can happen if your IAM policies contain wildcards (*) and are too broad to meet the control. In this case, you can update your IAM policies so that they don't allow full administrative privileges. To achieve this, you can determine what tasks users need to do, and then craft policies that let the users perform only those tasks. This corrective action helps to bring your AWS environment in line with FSBP requirements.

When your IAM policies are in line with the control, mark the control as *Reviewed* and add the evidence to your assessment report. You can then share this report with auditors to demonstrate that the control is working as intended.

Automated controls that use AWS Config as a data source type

This example shows a control that uses AWS Config as its data source type. This is a standard control taken from the [AWS Control Tower Guardrails framework](#). Audit Manager uses this control to generate evidence that helps bring your AWS environment in line with AWS Control Tower Guardrails.

Example control details

- **Control name** – 4.1.2 - Disallow public write access to S3 buckets
- **Control set** – This control belongs to the Disallow public access control set. This is a grouping of controls that relate to access management.
- **Data source type** – AWS Config
- **Evidence type** – Compliance check

In the following example, this control is within an Audit Manager assessment that was created from the AWS Control Tower Guardrails framework.

Control sets (1/5)		1 match			Delegate control set	Complete control set review
		Controls grouped by control set	Control status	Delegated to	Total evidence	Added to assessment report
○	▼ Disallow public access (4)	Active	-	0	0	
	4.1.2 - Disallow public write access to S3 buckets	Under review	-	0	0	

The assessment shows the control status, how much evidence was collected for this control so far, and how much of that evidence is included in your assessment report. From here, you can delegate the control set for review or complete the review yourself. Choosing the control name opens a detail page with more information, including the evidence for that control.

What this control does

Audit Manager can use this control to check if the access levels of your S3 bucket policies are too lenient to meet AWS Control Tower requirements. More specifically, it can check the Block Public Access settings, the bucket policies, and the bucket access control lists (ACL) to confirm that your buckets don't allow public write access.

How Audit Manager collects evidence for this control

Audit Manager takes the following steps to collect evidence for this control:

1. For each control, Audit Manager assesses your in-scope resources using the data source that's specified in the control settings. In this case, your S3 buckets are the resource, and AWS Config is the data source type. Audit Manager looks for the result of a specific AWS Config Rule ([s3-bucket-public-write-prohibited](#)) to evaluate the settings, policy, and ACL of each of the S3 buckets that are in scope of your assessment.
2. The result of the resource assessment is saved and converted into auditor-friendly evidence. Audit Manager generates *compliance check* evidence for controls that use AWS Config as a data source type. This evidence contains the result of the compliance check reported directly from AWS Config.
3. Audit Manager attaches the saved evidence to the control in your assessment that's named 4.1.2 - Disallow public write access to S3 buckets.

How you can use Audit Manager to demonstrate compliance with this control

After the evidence is attached to the control, you—or a delegate of your choice—can review the evidence to see if any remediation is necessary.

In this example, Audit Manager might display a ruling from AWS Config stating that an S3 bucket is *noncompliant*. This could happen if one of your S3 buckets has a Block Public Access setting that doesn't restrict public policies, and the policy that's in use allows public write access. To remediate this, you can update the Block Public Access setting to restrict public policies. Or, you can use a different bucket policy that doesn't allow public write access. This corrective action helps to bring your AWS environment in line with AWS Control Tower requirements.

When you're satisfied that your S3 bucket access levels are in line with the control, you can mark the control as *Reviewed* and add the evidence to your assessment report. You can then share this report with auditors to demonstrate that the control is working as intended.

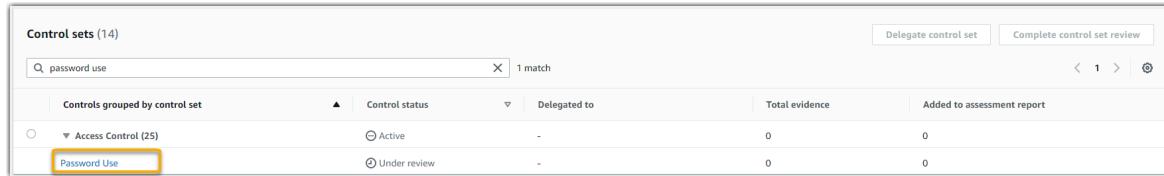
Automated controls that use AWS API calls as a data source type

This example shows a custom control that uses AWS API calls as its data source type. Audit Manager uses this control to generate evidence that can help to bring your AWS environment in line with your specific requirements.

Example control details

- **Control name** – Password Use
- **Control set** – This control belongs to a control set that's called Access Control. This is a grouping of controls that relate to identity and access management.
- **Data source type** – AWS API calls
- **Evidence type** – Configuration data

In the following example, this control is within an Audit Manager assessment that was created from a custom framework.



The screenshot shows a table titled "Control sets (14)" with a search bar at the top containing "Q: password use" which has found "1 match". The table has columns: "Controls grouped by control set", "Control status", "Delegated to", "Total evidence", and "Added to assessment report". There are two rows: one for "Access Control (25)" with status "Active" and "Under review", and another for "Password Use" which is currently selected and highlighted with a yellow border. The "Under review" status is indicated by a small orange circle icon.

Controls grouped by control set	Control status	Delegated to	Total evidence	Added to assessment report
Access Control (25)	Active	-	0	0
Password Use	Under review	-	0	0

The assessment shows the control status. It also shows how much evidence was collected for this control so far and how much of that evidence is included in your assessment report. From here, you can delegate the control set for review or complete the review yourself. Choosing the control name opens a detail page with more information, including the evidence for that control.

What this control does

Audit Manager can use this custom control to help you ensure that you have sufficient access control policies in place. This control requires that you follow good security practices in the selection and use of passwords. Audit Manager can help you to validate this by retrieving a list of all password policies for the IAM principals that are in the scope of your assessment.

How Audit Manager collects evidence for this control

Audit Manager takes the following steps to collect evidence for this custom control:

1. For each control, Audit Manager assesses your in-scope resources using the data source that's specified in the control settings. In this case, your IAM principals are the resources, and AWS API calls is the data source type. Audit Manager looks for the result of a specific IAM API call ([GetAccountPasswordPolicy](#)). It then returns the password policies for the AWS accounts that are in scope of your assessment.
2. The result of the resource assessment is saved and converted into auditor-friendly evidence. Audit Manager generates *configuration data* evidence for controls that use API calls as a data source. This evidence contains the original data that's captured from the API responses, and additional metadata that indicates which control the data supports.
3. Audit Manager attaches the saved evidence to the custom control in your assessment that's named Password Use.

How you can use Audit Manager to demonstrate compliance with this control

After the evidence is attached to the control, you—or a delegate of your choice—can review the evidence to see if it's sufficient or if any remediation is necessary.

In this example, you can review the evidence to see the responses from the API call. The [GetAccountPasswordPolicy](#) response describes the complexity requirements and mandatory rotation periods for the user passwords in your account. You can use this API response as evidence to show that you have sufficient password access control policies in place for the AWS accounts that are in the scope of your assessment. If you want, you can also provide additional commentary about these policies by adding a comment to the control.

When you're satisfied that the password policies of your IAM principals are in line with the custom control, you can mark the control as *Reviewed* and add the evidence to your assessment report. You can then share this report with auditors to demonstrate that the control is working as intended.

Automated controls that use AWS CloudTrail as a data source type

This example shows a control that uses AWS CloudTrail as its data source type. This is a standard control taken from the [HIPAA framework](#). Audit Manager uses this control to generate evidence that can help to bring your AWS environment in line with HIPAA requirements.

Example control details

- Control name** – 164.308(a)(5)(ii)(C)
- Control set** – This control belongs to the control set that's called 164.308 Administrative Safeguards.
- Data source type** – AWS CloudTrail
- Evidence type** – User activity

Here's this control shown within an Audit Manager assessment that was created from the HIPAA framework:

Control sets (6)				Delegate control set	Complete control set review
Q: 164.308(a)(5)(ii)(C)		X 1 match		< 1 > ⓘ	
Controls grouped by control set		Control status	Delegated to	Total evidence	Added to assessment report
○	▼ 164.308 Administrative Safeguards (22)	Active	-	0	0
	164.308(a)(5)(ii)(C)	Under review	-	0	0

The assessment shows the control status. It also shows how much evidence was collected for this control so far and how much of that evidence is included in your assessment report. From here, you can delegate the control set for review or complete the review yourself. Choosing the control name opens a detail page with more information, including the evidence for that control.

What this control does

This control requires a monitoring procedure for detecting inappropriate sign-ins. An example of an inappropriate sign-in is when someone enters multiple combinations of user names or passwords to attempt to access an information system. Audit Manager helps you to validate this control by providing a list of all detected sign-in attempts for the resources that are in the scope of your assessment.

How Audit Manager collects evidence for this control

Audit Manager takes the following steps to collect evidence for this control:

1. For each control, Audit Manager assesses your in-scope resources using the data source that's specified in the control settings. In this case, your users are the resource, and CloudTrail is the data source type. Audit Manager looks for the result of all [AWS Management Console sign-in events](#) that are logged by CloudTrail. It then returns a log of the relevant events that are within the scope of your assessment.
2. The result of the resource assessment is saved and converted into auditor-friendly evidence. Audit Manager generates *user activity* evidence for controls that use CloudTrail as a data source type. This evidence contains the original data that's captured from your users, and additional metadata that indicates which control the data supports.
3. Audit Manager attaches the saved evidence to the control in your assessment that's named 164.308(a)(5)(ii)(C).

How you can use Audit Manager to demonstrate compliance with this control

After the evidence is attached to the control, you—or a delegate of your choice—can review the evidence to see if any remediation is necessary.

In this example, you can review the evidence to see the sign-in events that were logged by CloudTrail. This log describes the console sign-in activity for your users, which includes the following information:

- Every successful sign-in
- Every unsuccessful sign-in attempt
- Verification of when multi-factor authentication (MFA) was enforced
- The IP address of every sign-in event

You can use this log as evidence to show that you have sufficient monitoring procedures in place for the AWS accounts that are in the scope of your assessment. If you like, you can also provide additional commentary by adding a comment to the control. For example, if the log shows any discrepancies such as multiple unsuccessful sign-in attempts, you can add a comment that describes how you remediated the issue. Regular monitoring of console sign-ins helps you to prevent security problems that may arise from discrepancies and inappropriate sign-in attempts. In turn, this best practice helps to bring your AWS environment in line with HIPAA requirements.

When you're satisfied that your monitoring procedure is in line with the control, you can mark the control as *Reviewed* and add the evidence to your assessment report. You can then share this report with auditors to demonstrate that the control is working as intended.

Manual controls

Some controls don't support automated evidence collection. This includes controls that rely on the provision of physical records and signatures, in addition to observations, interviews, and other events that aren't generated in the cloud. In these cases, you can manually upload evidence to demonstrate that you're satisfying the requirements of the control.

This example shows a manual control that Audit Manager doesn't collect automated evidence for. This is a standard control taken from the [NIST 800-53 \(Rev. 5\) framework](#). You can use Audit Manager to upload and store evidence that demonstrates compliance for this control.

Example control details

- **Control name** – PS-4(1) - Post-employment Requirements
- **Control set** – This control belongs to the Personnel Termination control set. This is a grouping of controls that relate to information security in the context of employment termination procedures.
- **Data source type** – Manual

- **Evidence type – Manual**

Here's this control shown within an Audit Manager assessment that was created from the NIST 800-53 (Rev. 5) Low-Moderate-High framework:

Control sets (1/280)				Delegate control set	Complete control set review
Controls grouped by control set		Control status	Delegated to	Total evidence	Added to assessment report
○	▼ Personnel Termination (3)	⌚ Active	-	0	0
	PS-4(1) - Post-employment Requirements	⌚ Under review	-	0	0

The assessment shows the control status. It also shows how much evidence was collected for this control so far and how much of that evidence is included in your assessment report. From here, you can delegate the control set for review or complete the review yourself. Choosing the control name opens a detail page with more information, including the evidence for that control.

What this control does

You can use this control to confirm that you're protecting organizational information if an employee is terminated. Specifically, you can demonstrate that you consistently notify terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information. Moreover, you can demonstrate that all terminated individuals sign an acknowledgment of post-employment requirements as part of the termination process for your organization.

How you can manually upload evidence for this control

You can take the following steps to upload manual evidence that supports this control:

1. Place the manual evidence that you want to upload in an Amazon Simple Storage Service (S3) bucket and note the S3 URI.
2. In your Audit Manager assessment, open the control, go to the evidence folders tab, and upload evidence by entering the S3 URI. For instructions, see [Uploading manual evidence in AWS Audit Manager](#).
3. Audit Manager creates an evidence folder that's named after the date when you upload the evidence. It then attaches the uploaded evidence to the control in your assessment that's named PS-4(1) - Post-employment Requirements.

How you can use Audit Manager to demonstrate compliance with this control

If you have documentation that supports this control, you can upload it as manual evidence. For example, you can upload the latest copy of legally binding post-employment requirements that your Human Resources department issues to terminated employees. If any individuals were terminated during the audit period, you could also upload dated copies that were addressed to those terminated individuals.

Much like with automated controls, you can delegate manual controls to stakeholders who can help you to review evidence (or, in this case, supply it). For example, when you review this control, you might realize that you only partially meet its requirements. This could be the case if you don't have an acknowledgement letter that was signed by a terminated individual. You could delegate the control to an HR stakeholder, who can then upload a copy of the signed letter. Or, if no employees were terminated during the audit period, you can leave a comment that states why no signed letters are attached to the control.

When you're satisfied that you're in line with the control, you can mark it as *Reviewed* and add the evidence to your assessment report. You can then share this report with auditors to demonstrate that the control is working as intended.

Controls with mixed data source types (automated and manual)

In many cases, a combination of automated and manual evidence is needed to satisfy a control. Although Audit Manager can provide automated evidence that's relevant to the control, you might need to supplement this data with manual evidence that you identify and upload yourself.

This example shows a control that uses a combination of manual evidence and automated evidence that comes from AWS API calls. This is a standard control taken from the [NIST 800-53 \(Rev. 5\) framework](#). Audit Manager uses this control to generate evidence that can help to bring your AWS environment in line with NIST requirements.

Example control details

- **Control name** – MA-5(3) - Citizenship Requirements for Classified Systems
- **Control set** – This control belongs to the Maintenance Personnel control set. This is a grouping of controls that relate to the individuals who perform hardware or software maintenance on organizational systems.
- **Data source type** – AWS API calls, plus supplemental manual evidence
- **Evidence type** – Configuration data

Here's this control shown within an Audit Manager assessment that was created from the NIST 800-53 (Rev. 5) framework:

Control sets (280)		Delegate control set		Complete control set review	
Controls grouped by control set		Control status	Delegated to	Total evidence	Added to assessment report
○	▼ Maintenance Personnel (6)	⌚ Active	-	0	0
	MA-5(3) - Citizenship Requirements for Classified Systems	⌚ Under review	-	0	0

The assessment shows the control status. It also shows how much evidence was collected for this control so far and how much of that evidence is included in your assessment report. From here, you can delegate the control set for review or complete the review yourself. Choosing the control name opens a detail page with more information, including the evidence for that control.

What this control does

Audit Manager can use this control to help you ensure that the personnel who perform your maintenance and diagnostic activities have the required citizenship status. If your system processes, stores, or transmits classified information, you must demonstrate that your maintenance personnel are U.S. citizens. Audit Manager helps you to validate this. It does this by returning a complete list of all the IAM policies and principals that are in the scope of your assessment. You can then verify and demonstrate that this list of users has the necessary citizenship requirements. You can do this by manually uploading supplemental evidence of their citizenship status.

How Audit Manager collects evidence for this control

Audit Manager takes the following steps to collect evidence for this control:

1. For each control, Audit Manager assesses your in-scope resources using the data source that's specified in the control settings. In this case, your IAM policies and principals are the resources, and AWS API calls is the data source. Audit Manager looks for the result of four specific IAM API calls ([ListUsers](#)/[ListRoles](#)/[ListGroups](#)/[ListPolicies](#)) and returns a list of the IAM policies and principals that are in scope of your assessment.

2. The result of the resource assessment is saved and converted into auditor-friendly evidence. Audit Manager generates *configuration data* evidence for controls that use API calls as a data source type. This evidence contains the original data that's captured from the API responses, and additional metadata that indicates which control the data supports.
3. Audit Manager attaches the saved evidence to the control in your assessment that's named MA-5(3) - Citizenship Requirements for Classified Systems.

How you can manually upload evidence for this control

You can take the following steps to upload manual evidence that supplements the automated evidence:

1. Place the documentation of citizenship in an Amazon Simple Storage Service (Amazon S3) bucket and note the S3 URI.
2. In your Audit Manager assessment, open the control, go to the evidence folders tab, and upload evidence. You do this by entering the S3 URI. For instructions, see [Adding manual evidence in AWS Audit Manager](#).
3. Audit Manager attaches the uploaded evidence to the control in your assessment that's named MA-5(3) - Citizenship Requirements for Classified Systems.

How you can use Audit Manager to demonstrate compliance with this control

After the evidence is attached to the control, you—or a delegate of your choice—can review the evidence to see if it's sufficient or if any remediation is necessary.

In this example, you might review the evidence and see a list of 20 users. If you're not sure how to identify which users are maintenance personnel, or the citizenship of those users, you can delegate the control to a subject matter expert for validation. The delegate can confirm the list of maintenance personnel, and upload supplemental evidence manually as documentation of their citizenship status. Confirming the citizenship of all the relevant listed users helps to bring your AWS environment in line with NIST requirements. Alternatively, if your system doesn't process, store, or transmit classified information, you can leave a comment that states why this control isn't applicable.

When you're satisfied that you're in line with the control, mark the control as *Reviewed* and add the evidence to your assessment report. You can then share this report with auditors to demonstrate that the control is working as intended.

Integrations with related AWS services

AWS Audit Manager integrates with multiple AWS services to automatically collect evidence that you can include in your assessment reports.

AWS Security Hub

AWS Security Hub monitors your environment using automated security checks that are based on AWS best practices and industry standards. Audit Manager captures snapshots of your resource security posture by reporting the results of security checks directly from Security Hub. For more information about Security Hub, see [What is AWS Security Hub?](#) in the *AWS Security Hub User Guide*.

AWS CloudTrail

AWS CloudTrail helps you monitor the calls made to AWS resources in your account. These include calls made by the AWS Management Console, the AWS CLI, and other AWS services. Audit Manager collects log data from CloudTrail directly, and converts the processed logs into user activity evidence. For more information about CloudTrail, see [What is AWS CloudTrail?](#) in the *AWS CloudTrail User Guide*.

AWS Config

AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. This includes information about how resources are related to one another and how they were configured in the past. Audit Manager captures snapshots of your resource security posture by reporting findings directly from AWS Config. For more information about AWS Config, see [What is AWS Config?](#) in the [AWS Config User Guide](#).

AWS License Manager

AWS License Manager streamlines the process of bringing software vendor licenses to the cloud. As you build out cloud infrastructure on AWS, you can save costs by repurposing your existing license inventory for use with cloud resources. Audit Manager provides a License Manager framework to assist you with your audit preparation. This framework is integrated with License Manager to aggregate license usage information based on customer defined licensing rules. For more information on License Manager, see [What is AWS License Manager?](#) in the [AWS License Manager User Guide](#).

AWS Control Tower

AWS Control Tower enforces preventative and detective guardrails for cloud infrastructure. Audit Manager provides an AWS Control Tower Guardrails framework to assist you with your audit preparation. This framework contains all of the AWS Config rules that are based on guardrails from AWS Control Tower. For more information about AWS Control Tower, see [What is AWS Control Tower?](#) in the [AWS Control Tower User Guide](#).

AWS Artifact

AWS Artifact is a self-service audit artifact retrieval portal that provides on-demand access to the compliance documentation and certifications for AWS infrastructure. AWS Artifact offers evidence to prove that the AWS Cloud infrastructure meets the compliance requirements. In contrast, AWS Audit Manager helps you collect, review, and manage evidence to demonstrate that your usage of AWS services is in compliance. For more information about AWS Artifact, see [What is AWS Artifact?](#) in the [AWS Artifact User Guide](#). You can download a [list of AWS reports](#) in the AWS Management Console.

For a list of AWS services in scope of specific compliance programs, see [AWS services in Scope by Compliance Program](#). For more general information, see [AWS Compliance Programs](#).

Integrations with third-party GRC products

AWS Audit Manager supports integrations with the third-party partner GRC products that are listed on this page.

If your company uses a hybrid cloud model or multicloud model, it's likely that you use a GRC product to manage evidence from those environments. When that product is integrated with Audit Manager, you can pull evidence about your AWS usage directly into your GRC environment. This simplifies how you manage compliance by providing you with a centralized place to review and remediate evidence as you prepare for audits.

Read this page for an overview of the third-party GRC products that can ingest evidence from Audit Manager. You can also see a reference of which Audit Manager API actions you can take directly within those products.

Topics

- [Understanding how third-party integrations work with Audit Manager \(p. 23\)](#)
- [Third-party GRC partner products that integrate with Audit Manager \(p. 23\)](#)

Understanding how third-party integrations work with Audit Manager

GRCA partners can use the Audit Manager public APIs to integrate their products with Audit Manager. With this integration in place, you can map the enterprise controls in your GRC environment to the controls that Audit Manager provides.

After you complete this one-time control mapping exercise, you can create Audit Manager assessments directly in the GRC product. This action starts the collection of evidence about your AWS usage. You can then see this AWS evidence along with the other evidence that's collected from your hybrid environment, all within the same context of your enterprise controls.

When you use an Audit Manager integration with a third-party GRC product, keep in mind the following points:

- Integrations are available for all [AWS Regions where Audit Manager is supported](#).
- Any Audit Manager resources that you create in the GRC partner product are also reflected in Audit Manager.
- You're subject to [AWS Audit Manager pricing](#) in addition to the pricing of the third-party GRC product.
- The evidence that Audit Manager collects is immutable. Evidence is presented in exactly the same way in third-party GRC products as it is in the Audit Manager console. However, if you use a third-party integration, you might be able to enhance this evidence by providing additional context in your reporting.
- The same [quotas that apply to Audit Manager](#) also apply within the third-party GRC product. For example, each AWS account can have up to 100 active Audit Manager assessments. This account-level quota applies whether you create the assessments in the Audit Manager console or in the third-party GRC product. Most Audit Manager quotas, but not all, are listed under the AWS Audit Manager namespace in the Service Quotas console. To learn how to request a quota increase, see [Managing your Audit Manager quotas \(p. 308\)](#).

If you have a compliance solution and you're interested in integrating with Audit Manager, email auditmanager-partners@amazon.com.

Third-party GRC partner products that integrate with Audit Manager

The following third party GRC products can ingest evidence from Audit Manager.

MetricStream

To use this integration, reach out to [MetricStream](#) for the access and purchase of MetricStream GRC software.

Built on the MetricStream Platform, the MetricStream Enterprise GRC solution allows for a comprehensive and collaborative approach to enterprise-wide GRC activities and processes. By ingesting evidence from Audit Manager into MetricStream, you can proactively identify non-compliant evidence from your AWS environment and review it alongside evidence from your on-premises data sources or other cloud partners. This provides you with a convenient and centralized way to review and improve your cloud security and compliance posture as you prepare for audits.

With the MetricStream and Audit Manager integration, you can perform the following API operations.

Task	API operation
Setting up the Audit Manager integration	<ul style="list-style-type: none"> • GetAccountStatus • GetOrganizationAdminAccount • GetSettings
Reviewing Audit Manager resources	<ul style="list-style-type: none"> • GetAssessment • GetAssessmentFramework • GetControl • ListAssessmentFrameworks • ListControls
Creating Audit Manager resources	<ul style="list-style-type: none"> • CreateAssessment • CreateAssessmentFramework
Updating Audit Manager resources	<ul style="list-style-type: none"> • UpdateAssessment • UpdateAssessmentControl • UpdateAssessmentStatus
Managing evidence	<ul style="list-style-type: none"> • StartQuery (AWS CloudTrail API) • GetQueryResults (AWS CloudTrail API)
Deleting Audit Manager resources	<ul style="list-style-type: none"> • DeleteAssessmentFramework

Related MetricStream links

- [AWS Marketplace link](#)
- [Product link](#)
- [Product pricing](#)

Using Audit Manager with an AWS SDK

AWS software development kits (SDKs) are available for many popular programming languages. Each SDK provides an API, code examples, and documentation that developers can use to build applications in their preferred language.

SDK documentation	Audit Manager specific documentation	Code examples	
AWS SDK for C++	AWS SDK for C++ API reference for Audit Manager	AWS SDK for C++ code examples	
AWS SDK for Go	AWS SDK for Go API reference for Audit Manager	AWS SDK for Go code examples	
AWS SDK for Java	AWS SDK for Java 2.x API reference for Audit Manager	AWS SDK for Java code examples	
AWS SDK for JavaScript	AWS SDK for JavaScript API reference for Audit Manager	AWS SDK for JavaScript code examples	

SDK documentation	Audit Manager specific documentation	Code examples	
AWS SDK for .NET	AWS SDK for .NET API reference for Audit Manager	AWS SDK for .NET code examples	
AWS SDK for PHP	AWS SDK for PHP API reference for Audit Manager	AWS SDK for PHP code examples	
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto) API reference for Audit Manager	AWS SDK for Python (Boto3) code examples	
AWS SDK for Ruby	AWS SDK for Ruby API reference for Audit Manager	AWS SDK for Ruby code examples	

For examples that are specific to Audit Manager, see [Code examples for AWS Audit Manager](#).

Note

Audit Manager is available in botocore version 1.19.32 and later for the AWS SDK for Python (Boto3). Before you start using the SDK, make sure that you're using the appropriate botocore version.

Setting up AWS Audit Manager

Before you start using Audit Manager, ensure that you completed the following setup tasks.

Topics

- [Prerequisites: Create an AWS account and set up permissions](#)
- [Enable Audit Manager: Use the console, the AWS CLI, or the API to enable Audit Manager](#)
- [Recommendations: Set up recommended integrations with other AWS services](#)

Prerequisites

Follow these steps to create an AWS account and an administrative user with Audit Manager setup privileges.

Steps

- [Sign up for an AWS account \(p. 26\)](#)
- [Create an administrative user \(p. 26\)](#)
- [Add the required permissions to access and enable Audit Manager \(p. 27\)](#)

Important

If you're already set up with AWS and IAM, you can skip steps 1 and 2. However, you must complete step 3 to ensure that you have the required permissions to set up Audit Manager.

Sign up for an AWS account

If you do not have an AWS account, complete the following steps to create one.

To sign up for an AWS account

1. Open <https://portal.aws.amazon.com/billing/signup>.
2. Follow the online instructions.

Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

When you sign up for an AWS account, an *AWS account root user* is created. The root user has access to all AWS services and resources in the account. As a security best practice, [assign administrative access to an administrative user](#), and use only the root user to perform [tasks that require root user access](#).

AWS sends you a confirmation email after the sign-up process is complete. At any time, you can view your current account activity and manage your account by going to <https://aws.amazon.com/> and choosing **My Account**.

Create an administrative user

After you sign up for an AWS account, create an administrative user so that you don't use the root user for everyday tasks.

Secure your AWS account root user

1. Sign in to the [AWS Management Console](#) as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.

For help signing in by using root user, see [Signing in as the root user](#) in the *AWS Sign-In User Guide*.

2. Turn on multi-factor authentication (MFA) for your root user.

For instructions, see [Enable a virtual MFA device for your AWS account root user \(console\)](#) in the *IAM User Guide*.

Create an administrative user

- For your daily administrative tasks, grant administrative access to an administrative user in AWS IAM Identity Center.

For instructions, see [Getting started](#) in the *AWS IAM Identity Center User Guide*.

Sign in as the administrative user

- To sign in with your IAM Identity Center user, use the sign-in URL that was sent to your email address when you created the IAM Identity Center user.

For help signing in using an IAM Identity Center user, see [Signing in to the AWS access portal](#) in the *AWS Sign-In User Guide*.

Add the required permissions to access and enable Audit Manager

You must give users the required permissions to enable Audit Manager. For users who need full access to Audit Manager, use the [AWSAuditManagerAdministratorAccess](#) managed policy. This is an AWS managed policy that's available in your AWS account, and it's the recommended policy for Audit Manager administrators.

Tip

As a security best practice, we recommend that you get started with AWS managed policies and then move toward least-privilege permissions. AWS managed policies grant permissions for many common use cases. However, keep in mind that because AWS managed policies are available for use by all AWS customers, they might not grant least-privilege permissions for your specific use cases. As a result, we recommend that you reduce permissions further by defining [customer managed policies](#) that are specific to your use cases. For more information, see [AWS managed policies](#) in the *AWS Identity and Access Management User Guide*.

To provide access, add permissions to your users, groups, or roles:

- Users and groups in AWS IAM Identity Center:

Create a permission set. Follow the instructions in [Create a permission set](#) in the *AWS IAM Identity Center User Guide*.

- Users managed in IAM through an identity provider:

Create a role for identity federation. Follow the instructions in [Creating a role for a third-party identity provider \(federation\)](#) in the *IAM User Guide*.

- IAM users:

- Create a role that your user can assume. Follow the instructions in [Creating a role for an IAM user](#) in the *IAM User Guide*.
- (Not recommended) Attach a policy directly to a user or add a user to a user group. Follow the instructions in [Adding permissions to a user \(console\)](#) in the *IAM User Guide*.

Enable AWS Audit Manager

You can enable Audit Manager using the AWS Management Console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI).

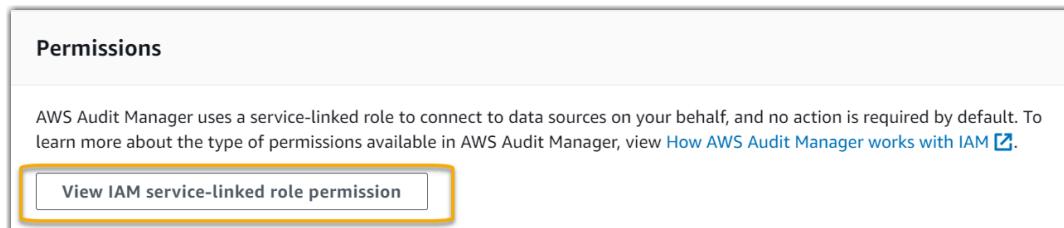
Audit Manager console

To enable Audit Manager using the console

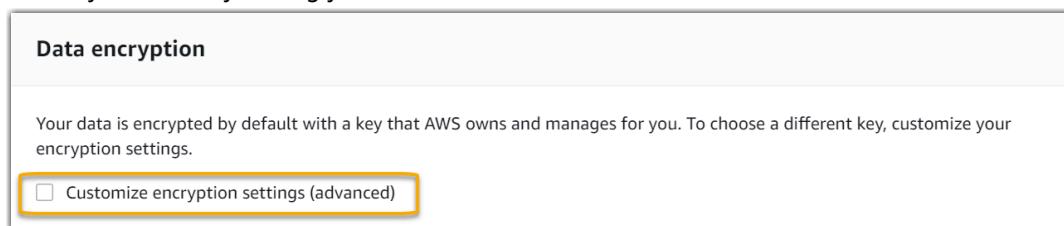
1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. Use the credentials of your IAM identity to sign in.
3. Choose **Set up AWS Audit Manager**.



4. Under **Permissions**, no action is required. This is because Audit Manager uses a [service-linked role](#) to connect to data sources on your behalf. You can review the service-linked role by choosing **View IAM service-linked role permission**.



5. Under **Data encryption**, the default option is for Audit Manager to create and manage an AWS KMS key for securely storing your data.



If you want to use your own customer managed key to encrypt data in Audit Manager, select the check box next to **Customize encryption settings (advanced)**. You can then choose an existing KMS key or [create a new one](#).

Data encryption

Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.

- Customize encryption settings (advanced)
To use the default key, clear this option.

Choose an AWS KMS key

This key will be used for encryption instead of the default key.

Choose an AWS KMS key or enter an ARN

[Create an AWS KMS key](#)

6. (Optional) Under **Delegated administrator - optional**, you can specify a delegated administrator account if you want Audit Manager to run assessments for multiple accounts. For more information and recommendations, see [Enable and set up AWS Organizations for use with Audit Manager](#).

Delegated administrator - *optional*

For AWS Audit Manager to support multiple accounts in your organization, you must specify a delegated administrator. Use this setting to add or remove the delegated AWS Audit Manager administrator for your organization. [Learn more](#)

Delegated administrator account ID

123456789012

[Delegate](#)

7. (Optional) Under **AWS Config – optional**, we recommend that you enable AWS Config for an optimal experience. This enables Audit Manager to generate evidence using AWS Config rules. For instructions and recommended settings, see [Enable and set up AWS Config for use with Audit Manager](#).

AWS Config - *optional*

Allow AWS Audit Manager to access [AWS Config](#) and generate evidence from AWS Config rules. Enabling AWS Config incurs charges.

[Enable AWS Config](#)

8. (Optional) Under **Security Hub – optional**, we recommend that you enable Security Hub for an optimal experience. This enables Audit Manager to generate evidence using Security Hub checks. For instructions and recommended settings, see [Enable and set up AWS Security Hub for use with Audit Manager](#).

Security Hub - *optional*

Allow AWS Audit Manager to access [Security Hub](#) and generate evidence from security findings. Enabling Security Hub incurs charges.

[Enable Security Hub](#)

9. Choose **Complete setup** to finish the setup process.

[Complete setup](#)

AWS CLI

To enable Audit Manager using the AWS CLI

In the command line, run the [register-account](#) command using the following setup parameters:

- **--kms-key** (optional) – Use this parameter to encrypt your Audit Manager data using your own customer managed key. If you don't specify an option here, Audit Manager creates and manages an AWS KMS key on your behalf for the secure storage of your data.
- **--delegated-admin-account** (optional) – Use this parameter to designate your organization's delegated administrator account for Audit Manager. If you don't specify an option here, no delegated administrator is registered.

Input example (replace the *placeholder text* with your own information):

```
aws auditmanager register-account \
--kms-key arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
--delegated-admin-account 111122224444
```

Output example:

```
{  
    "status": "ACTIVE"  
}
```

For more information about the AWS CLI and for instructions on installing the AWS CLI tools, see the following in the *AWS Command Line Interface User Guide*.

- [AWS Command Line Interface User Guide](#)
- [Getting Set Up with the AWS Command Line Interface](#)

Audit Manager API

To enable Audit Manager using the Audit Manager API

Use the [RegisterAccount](#) operation with the following setup parameters:

- **kmsKey** (optional) – Use this parameter to encrypt your Audit Manager data using your own customer managed key. If you don't specify an option here, Audit Manager creates and manages an AWS KMS key on your behalf for the secure storage of your data.
- **delegatedAdminAccount** (optional) – Use this parameter to specify your organization's delegated administrator account for Audit Manager. If you don't specify one, no delegated administrator is registered.

Input example (replace the *placeholder text* with your own information):

```
{  
    "kmsKey": "arn:aws:kms:us-  
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",  
    "delegatedAdminAccount": "111122224444"  
}
```

Output example:

```
{
```

```
    "status": "ACTIVE"  
}
```

Recommendations

For an optimal experience in Audit Manager, we recommend that you set up the following features and enable the following AWS services.

Topics

- [Set up recommended Audit Manager features \(p. 31\)](#)
- [Set up recommended integrations with other AWS services \(p. 31\)](#)

Set up recommended Audit Manager features

After you enable Audit Manager, we recommend that you enable the evidence finder feature.

[Evidence finder \(p. 90\)](#) provides a powerful way to search for evidence in Audit Manager. Instead of browsing deeply nested evidence folders to find what you're looking for, you can use evidence finder to quickly query your evidence. If you use evidence finder as a delegated administrator, you can search for evidence across all member accounts in your organization. Using a combination of filters and groupings, you can progressively narrow the scope of your search query. For example, if you want a high-level view of your system health, perform a broad search and filter by assessment, date range, and resource compliance. If your goal is to remediate a specific resource, you can perform a narrow search to target evidence for a specific control or resource ID. After you define your filters, you can group and then preview the matching search results before creating an assessment report.

To use evidence finder, you must enable this feature from your Audit Manager settings. For instructions, see [Evidence finder settings \(p. 263\)](#).

Set up recommended integrations with other AWS services

For an optimal experience in Audit Manager, we strongly recommend that you enable the following AWS services:

- **AWS Organizations** – You can use Organizations to run Audit Manager assessments over multiple accounts and consolidate evidence into a delegated administrator account.
- **AWS Security Hub and AWS Config** – When you enable these AWS services, they can be used as a data source type for the controls in your Audit Manager assessments. Audit Manager can then report the results of compliance checks directly from these services.

Topics

- [Enable and set up AWS Config \(optional\) \(p. 31\)](#)
- [Enable and set up AWS Security Hub \(optional\) \(p. 32\)](#)
- [Enable AWS Organizations \(optional\) \(p. 34\)](#)

Enable and set up AWS Config (optional)

Many controls in Audit Manager use AWS Config as a data source type. To support these controls, you must enable AWS Config on all accounts in each AWS Region where Audit Manager is enabled. If Audit

Manager tries to collect evidence for controls that use AWS Config as a data source type, and the related AWS Config rules aren't enabled, no evidence is collected for those controls.

Audit Manager doesn't manage AWS Config for you. You can follow these steps to enable AWS Config and configure its settings.

Tasks to integrate AWS Config with Audit Manager

- [Step 1: Enable AWS Config \(p. 32\)](#)
- [Step 2: Configure your AWS Config settings for use with Audit Manager \(p. 32\)](#)

Step 1: Enable AWS Config

You can enable AWS Config using the AWS Config console or API. For instructions, see [Getting started with AWS Config](#) in the *AWS Config Developer Guide*.

Step 2: Configure your AWS Config settings for use with Audit Manager

Important

Enabling AWS Config is an optional recommendation. However, if you do enable AWS Config, the following settings are required.

After you enable AWS Config, make sure that you also [enable AWS Config rules](#) or [deploy a conformance pack](#) for the compliance standard that's related to your audit. This step ensures that Audit Manager can import findings for the AWS Config rules that you enabled.

After you enable an AWS Config rule, we recommend that you review the parameters of that rule. You should then validate those parameters against the requirements of your chosen compliance framework. If needed, you can [update a rule's parameters in AWS Config](#) to ensure that it aligns with framework requirements. This will help to ensure that your assessments collect the correct compliance check evidence for a given framework.

For example, suppose that you're creating an assessment for CIS v1.2.0. This framework has a control named [1.4 – Ensure access keys are rotated every 90 days or less](#). In AWS Config, the [access-keys-rotated](#) rule has a maxAccessKeyAge parameter with a default value of 90 days. As a result, the rule aligns with the control requirements. If you aren't using the default value, ensure that the value you're using is equal to or greater than the 90 day requirement from CIS v1.2.0.

You can find the default parameter details for each managed rule in the [AWS Config documentation](#). For instructions on how to configure a rule, see [Working with AWS Config Managed Rules](#).

Enable and set up AWS Security Hub (optional)

Many controls in Audit Manager use Security Hub as a data source type. To support these controls, you must enable Security Hub on all accounts in each Region where Audit Manager is enabled. If Audit Manager tries to collect evidence for controls that use Security Hub as a data source type, and the related Security Hub standards aren't enabled, no evidence is collected for those controls.

Audit Manager doesn't manage Security Hub for you. You can follow these steps to enable Security Hub and configure its settings.

Tasks to integrate AWS Security Hub with Audit Manager

- [Step 1: Enable AWS Security Hub \(p. 33\)](#)
- [Step 2: Configure your Security Hub settings for use with Audit Manager \(p. 33\)](#)

Step 1: Enable AWS Security Hub

You can enable Security Hub using either the console or the API. For instructions, see [Setting up AWS Security Hub](#) in the *AWS Security Hub User Guide*.

Step 2: Configure your Security Hub settings for use with Audit Manager

Important

Enabling Security Hub is an optional recommendation. However, if you do enable Security Hub, the following settings are required.

After you enable Security Hub, make sure that you also do the following:

- [Enable AWS Config and configure resource recording](#) - Security Hub uses service-linked AWS Config rules to perform most of its security checks for controls. To support these controls, AWS Config must be enabled and configured to record resources that are required for the controls that you have enabled in each enabled standard.
- [Enable all security standards](#) - This step ensures that Audit Manager can import findings for all supported compliance standards.
- [Turn on the consolidated control findings setting in Security Hub](#) - This setting is turned *on* by default if you enable Security Hub on or after February 23, 2023.

Note

When you enable consolidated findings, Security Hub produces a single finding for each security check (even when the same check is used across multiple standards). Each Security Hub finding is collected as one unique resource assessment in Audit Manager. As a result, consolidated findings results in a decrease of the total unique resource assessments that Audit Manager performs for Security Hub findings. For this reason, using consolidated findings can often result in a reduction in your Audit Manager usages costs. For more information about using Security Hub as a data source type, see [AWS Security Hub controls supported by AWS Audit Manager \(p. 224\)](#). For more information about Audit Manager pricing, see [AWS Audit Manager Pricing](#).

If you use AWS Organizations and you want to collect Security Hub evidence from your member accounts, you must also perform the following steps in Security Hub.

To set up your organization's Security Hub settings

1. Sign in to the AWS Management Console and open the AWS Security Hub console at <https://console.aws.amazon.com/securityhub/>.
2. Using your AWS Organizations management account, designate an account as the delegated administrator for Security Hub. For more information, see [Designating a Security Hub administrator account](#) in the *AWS Security Hub User Guide*.

Note

Make sure that the delegated administrator account that you designate in Security Hub is the same one that you use in Audit Manager.

3. Using your Organizations delegated administrator account, go to **Settings, Accounts**, select all accounts, and then add them as members by selecting **Auto-enroll**. For more information, see [Enabling member accounts from your organization](#) in the *AWS Security Hub User Guide*.
4. Enable AWS Config for every member account of the organization. For more information, see [Enabling member accounts from your organization](#) in the *AWS Security Hub User Guide*.
5. Enable the PCI DSS security standard for every member account of the organization. The AWS CIS Foundations Benchmark standard and the AWS Foundational Best Practices standard are already enabled by default. For more information, see [Enabling a security standard](#) in the *AWS Security Hub User Guide*.

Enable AWS Organizations (optional)

Audit Manager supports multiple accounts via integration with AWS Organizations. Audit Manager can run assessments over multiple accounts and consolidate evidence into a delegated administrator account. The delegated administrator has permissions to create and manage Audit Manager resources with the organization as the zone of trust. Only the management account can designate a delegated administrator.

Tasks to integrate AWS Organizations with Audit Manager

- [Step 1: Create or join an organization \(p. 34\)](#)
- [Step 2: Enable all features in your organization \(p. 34\)](#)
- [Step 3: Specify a delegated administrator for Audit Manager \(p. 34\)](#)

Step 1: Create or join an organization

If your AWS account isn't part of an organization, you can create or join an organization. For instructions, see [Creating and managing an organization](#) in the *AWS Organizations User Guide*.

Step 2: Enable all features in your organization

Next, you must enable all features in your organization. For instructions, see [Enabling all features in your organization](#) in the *AWS Organizations User Guide*.

Step 3: Specify a delegated administrator for Audit Manager

We recommend that you enable Audit Manager using an Organizations management account, and then specify a delegated administrator. After that, you can use the delegated administrator account to log in and run assessments. As a best practice, we recommend that you only create assessments using the delegated administrator account instead of the management account.

Warning

After you specify a delegated administrator using an Organizations management account, your management account can no longer create additional assessments in Audit Manager.

Additionally, evidence collection stops for any existing assessments that were created by the management account. Instead, Audit Manager collects and attaches evidence to the delegated administrator, which is the main account for managing your organization's assessments.

To add or change a delegated administrator after you enable Audit Manager, see [AWS Audit Manager settings, Delegated administrator](#).

Issues to consider:

- You can't use your management account as a delegated administrator in Audit Manager.
- If you want to enable Audit Manager in more than one AWS Region, you must designate a delegated administrator account separately in each Region. In your Audit Manager settings, you should designate the same delegated administrator account across all Regions.
- If you provided a customer managed key when you enabled Audit Manager, make sure that the delegated administrator account has access on that KMS key. To review and change your Audit Manager encryption settings, see [Data encryption \(p. 252\)](#).
- For solutions to common Organizations and delegated administrator issues in Audit Manager, see [Troubleshooting delegated administrator and AWS Organizations issues \(p. 289\)](#).

What do I do next?

Now that you have set up Audit Manager, you're ready to get started with using the service. You can also visit the settings page of the console to update any of the settings that you chose when setting up Audit Manager.

Get started with Audit Manager

You can get started in Audit Manager by following a tutorial that walks you through how to create your first assessment. For more information, see [Tutorial for Audit Owners: Creating an assessment](#).

Update your Audit Manager settings

You can update your settings at any time. For more information, see [AWS Audit Manager settings \(p. 251\)](#).

Getting started with AWS Audit Manager

Use the step-by-step tutorials in this section to learn how to perform tasks using AWS Audit Manager.

Tip

The following tutorials are categorized by audience. Choose the tutorial that's appropriate for you based on your role as an *audit owner* or *delegate*.

- **Audit owners** are Audit Manager users who are responsible for creating and managing assessments. In the business world, audit owners are typically governance, risk management, and compliance (GRC) professionals. In the context of Audit Manager, however, individuals from SecOps or DevOps teams might also assume the user persona of an audit owner. Audit owners can request assistance from a subject matter expert—also known as a delegate—to review specific controls and validate evidence. Audit owners must have the necessary permissions to manage an assessment.
- **Delegates** are subject matter experts with specialized technical or business expertise. Although they don't own or manage Audit Manager assessments, they can still contribute to them. Delegates assist audit owners with tasks such as validating evidence for the controls that fall under their area of expertise. Delegates have limited permissions in Audit Manager. This is because audit owners delegate specific control sets for review, and not entire assessments.

For more information about these personas and other Audit Manager concepts, see *Audit owners* and *Delegates* in the [AWS Audit Manager concepts and terminology \(p. 2\)](#) section of this guide. For more information about the recommended IAM permissions for each persona, see [Recommended policies for user personas in AWS Audit Manager \(p. 317\)](#).

Audit Manager tutorials

[Creating an assessment](#)

Audience: Audit owners

Overview: Follow step-by-step instructions to create your first assessment and get up and running fast. This tutorial walks you through how you can use one a standard framework to create an assessment and begin the automated collection of evidence.

[Reviewing a control set](#)

Audience: Delegates

Overview: Assist an audit owner by reviewing evidence for controls that fall under your area of expertise. Learn to review control sets and their related evidence, add comments, upload additional evidence, and update the status of a control.

Tutorial for Audit Owners: Creating an assessment

This tutorial provides an introduction to AWS Audit Manager. In this tutorial, you create an assessment using the [AWS Audit Manager Sample Framework](#). By creating an assessment, you start the ongoing process of automated evidence collection for the controls in that framework.

This tutorial shows how to do the following:

- [Select a standard framework to create an assessment from](#)
- [Specify the AWS accounts to include in your assessment](#)
- [Specify the AWS services to include in your assessment](#)
- [Specify the audit owners for your assessment](#)
- [Review and create your assessment](#)

Before you start this tutorial, make sure that you first meet the following conditions:

- You completed all the prerequisites that are described in [Setting up AWS Audit Manager \(p. 26\)](#). You must use your AWS account and the AWS Audit Manager console to complete this tutorial.
- Your IAM identity is granted with the appropriate permissions to create and manage an assessment in AWS Audit Manager. Two suggested policies that grant these permissions are [Example 2: Allow full administrator access](#) and [Example 3: Allow management access](#).
- You're familiar with Audit Manager terminology and functionality. For a general overview, see [What is AWS Audit Manager? \(p. 1\)](#) and [AWS Audit Manager concepts and terminology \(p. 2\)](#).

Note

AWS Audit Manager assists in collecting evidence that's relevant for verifying compliance with specific compliance frameworks and regulations. However, it doesn't assess your compliance itself. The evidence that's collected through AWS Audit Manager therefore might not include all the information about your AWS usage that's needed for audits. AWS Audit Manager isn't a substitute for legal counsel or compliance experts.

Step 1: Specify assessment details

For the first step, select a framework and provide basic information for your assessment.

To specify assessment details

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. Choose **Launch AWS Audit Manager**.
3. In the navigation pane, choose **Getting Started**, and then choose **Start with a framework**.
4. Choose the framework that you want, and then choose **Create assessment from framework**. This example uses the **AWS Audit Manager Sample Framework**.
5. Under **Assessment name**, enter a name for your assessment.
6. (Optional) Under **Assessment description**, enter a description for your assessment.
7. Under **Assessment reports destination**, choose the Amazon S3 bucket where you want to save your assessment reports.
8. Under **Frameworks**, confirm that **AWS Audit Manager Sample Framework** (or the framework of your choice) is selected.
9. Under **Tags**, choose **Add new tag** to associate a tag with your assessment. You can specify a key and a value for each tag. The tag key is mandatory and can be used as a search criteria when you search for this assessment. For more information about tags in AWS Audit Manager, see [Tagging AWS Audit Manager resources \(p. 367\)](#).
10. Choose **Next**.

Step 2: Specify AWS accounts in scope

Next, specify the AWS accounts that you want to include in the scope of your assessment.

AWS Audit Manager integrates with AWS Organizations, so you can run an Audit Manager assessment across multiple accounts and consolidate evidence into a delegated administrator account. To enable Organizations in Audit Manager (if you didn't do so already), see [Enable AWS Organizations \(optional\) \(p. 34\)](#) on the *Setting up* page of this guide.

Note

Audit Manager can support up to approximately 150 accounts in the scope of an assessment. If you try to include over 150 accounts, the assessment creation might fail.

To specify accounts in scope

1. Under **AWS accounts**, select the AWS accounts that you want to include in the scope of your assessment.
 - If you enabled Organizations in AWS Audit Manager, multiple accounts are listed.
 - If you did not enable Organizations in Audit Manager, only your current account is listed.
2. Choose **Next**.

Step 3: Specify AWS services in scope

The framework that you selected earlier defines the AWS services that Audit Manager monitors and collects evidence for.

When you use the Audit Manager console to create an assessment from a standard framework, the list of services in scope is preselected and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the standard framework. If a listed AWS service isn't selected, Audit Manager doesn't collect evidence from resources related to that service. This is also the case if it's selected but you haven't subscribed to it in your environment.

In this step of the tutorial, you can review which AWS services are in the scope of the assessment based on the framework definition. To learn more about frameworks and how to access and review them, see the [Framework library \(p. 107\)](#) section of this guide.

To specify AWS services in scope

1. Under **AWS services**, review the list of services that are in scope for this assessment.
2. Choose **Next**.

Tip

If you need to edit the list of services in scope, you can do so by using the [CreateAssessment API](#) that's provided by Audit Manager.

Alternatively, you can [customize a standard framework](#) and then create an assessment from the custom framework.

Step 4: Specify audit owners

In this step, you specify the audit owners for your assessment. Audit owners are the individuals in your workplace—usually from GRC, SecOps, or DevOps teams—who are responsible for managing the Audit Manager assessment. We recommend that they use the [AWSAuditManagerAdministratorAccess](#) policy.

To specify audit owners

1. Under **Audit owners**, choose the audit owners for your assessment. To find additional audit owners, use the search bar to search by name or AWS account.
2. Choose **Next**.

Step 5: Review and create

Review the information for your assessment. To change the information for a step, choose **Edit**. When you're finished, choose **Create assessment** to launch your first assessment and start the ongoing collection of evidence.

After you create an assessment, evidence collection continues until you [change the assessment status to inactive](#). Alternatively, you can stop evidence collection for a specific control by [changing the control status to inactive](#).

Note

Automated evidence is available 24 hours after you create the assessment. AWS Audit Manager automatically collects evidence from multiple data sources, and the frequency of that evidence collection is based on the evidence type. For more information, see [Evidence collection frequency \(p. 12\)](#) in this guide.

Where do I go from here?

We recommend that you continue to learn more about the concepts and tools that are introduced in this tutorial. You can do so by reviewing the following resources:

- [Reviewing an assessment \(p. 56\)](#) – Introduces you to the assessment page where you can explore the different components of your assessment.
- [Assessments in AWS Audit Manager \(p. 50\)](#) – Builds upon this tutorial and provides in-depth information about the concepts and tasks for managing an assessment. In this document, we particularly recommend you check out these following topics:
 - How to [create an assessment](#) from a different framework
 - How to [review the evidence in an assessment](#) and [generate an assessment report](#)
 - How to [change the status of an assessment](#) or [delete an assessment](#)
- [Framework library \(p. 107\)](#) – Introduces the framework library and explains how to [create a custom framework](#) for your own specific compliance needs.
- [Control library \(p. 200\)](#) – Introduces the control library and explains how to [create a custom control](#) for use in your custom framework.
- [AWS Audit Manager concepts and terminology \(p. 2\)](#) – Provides definitions for the concepts and terminology used in Audit Manager.
- [Video] [Collect Evidence and Manage Audit Data Using AWS Audit Manager](#)– Shows the assessment creation process that's described in this tutorial, and other tasks such as reviewing a control and generating an assessment report.

Tutorial for Delegates: Reviewing a control set

This tutorial describes how to review a control set that was shared with you by an audit owner in AWS Audit Manager.

Audit owners use Audit Manager to create assessments and collect evidence for the controls listed in that assessment. Sometimes audit owners might have questions or need assistance when validating the evidence for a control set. In this situation, an audit owner can delegate a control set to a subject matter expert for review.

As a delegate, you help audit owners to review the collected evidence for controls that fall under your area of expertise.

This tutorial shows how to do the following:

- [Access notifications sent to you by an audit owner](#)
- [Review a control set and its related evidence](#)
- [Upload manual evidence to support a control](#)
- [Add a comment for a control that you're reviewing](#)
- [Update the status of a control](#)
- [Submit the reviewed control set to the audit owner when your review is complete](#)

Before you start this tutorial, make sure that you first meet the following conditions:

- Your AWS account is set up. To complete this tutorial, you must use both your AWS account and the AWS Audit Manager console. For more information, see [Setting up AWS Audit Manager \(p. 26\)](#).
- You're familiar with Audit Manager terminology and functionality. For a general overview of Audit Manager, see [What is AWS Audit Manager? \(p. 1\)](#) and [AWS Audit Manager concepts and terminology \(p. 2\)](#).

Step 1: Access your notifications

Start by signing in to AWS Audit Manager, where you can access your notifications to see the control sets that have been delegated to you for review.

To access your notifications

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the left navigation pane, choose **Notifications**. Or, in the blue flash bar at the top of the page, choose **View notification** to open the notifications page.
3. On the **Notifications** page, you review the list of control sets that have been delegated to you. The notifications table includes the following information:
 - **Date** – The date when the control set was delegated.
 - **Assessment** – The name of the assessment that's associated with the control set. You can choose an assessment name to open the assessment detail page.
 - **Control set** – The name of the control set that was delegated to you for review.
 - **Source** – The user or role that delegated the control set to you.
 - **Description** – The review instructions that were provided by the audit owner.

Tip

You can also subscribe to an SNS topic to receive email alerts when a control set is assigned to you for review. For more information, see [Notifications in AWS Audit Manager](#).

Step 2: Review the control set and related evidence

The next step is to review the control sets that the audit owner delegated to you. By examining the controls and their evidence, you can determine if any additional action is needed for a control. Additional actions can include manually uploading additional evidence to demonstrate compliance or leaving a comment about that control.

To review a control set

1. From the **Notifications** page, review the list of control sets that were delegated to you. Then identify which one you want to review and choose the name of the related assessment.

2. Under the **Controls** tab of the assessment detail page, scroll down to the **Control sets** table.
3. Under the **Controls grouped by control set** column, expand the name of a control set to show its controls. Then, choose the name of a control to open the control detail page.
4. (Optional) Choose **Update control status** to change the status of the control. While your review is in progress, you can mark the status as **Under Review**.
5. Review information about the control in the **Evidence folders**, **Data sources**, **Comments**, and **Changelog** tabs. For more information about each of these tabs and how to interpret the data that they contain, see [Review the controls in an assessment](#).

To review the evidence for a control

1. From the control detail page, choose the **Evidence folders** tab.
2. Navigate to the **Evidence folders** table, where a list of folders that contains evidence for that control is displayed. These folders are organized and named based on the date when the evidence within that folder was collected.
3. Choose the name of an evidence folder to open it. From here, you can review a summary of all the evidence that was gathered on that date. This summary also includes the total number of compliance check issues that were reported directly from AWS Security Hub, AWS Config, or both. For instructions on how to interpret the data on this page, see [Reviewing evidence folders](#).
4. From the evidence folder summary page, navigate to the **Evidence** table. Under the **Time** column, choose a line item to open and review details of the evidence that was collected at that time. For instructions on how to interpret the data on an evidence detail page, see [Reviewing individual evidence](#).

Step 3. Upload manual evidence (optional)

Although AWS Audit Manager automatically collects evidence for many controls, in some cases you might need to provide additional evidence. In these cases, you can manually upload evidence that helps you to demonstrate compliance with that control.

Before you can upload manual evidence to your assessment, you must first place the evidence in an S3 bucket. For instructions, see [Creating a bucket](#) and [Uploading objects](#) in the *Amazon Simple Storage Service User Guide*.

Important

Each AWS account can only manually upload up to 100 evidence files to a control each day. Exceeding this daily quota causes any additional manual uploads to fail for that control. If you need to upload a large amount of manual evidence to a single control, upload your evidence in batches across several days.

To upload manual evidence to a control

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. From the **Notifications** page, you can see the list of control sets that were delegated to you. Identify which control set you want to add evidence for, and choose the name of the related assessment to open the assessment detail page.
3. Choose the **Controls** tab, scroll down to **Control sets**, and then select the name of a control to open it.
4. Choose the **Evidence folders** tab, and then choose **Upload manual evidence**.
5. On the next page, enter the S3 URI of the evidence. You can find the S3 URI by navigating to the object in the [Amazon S3 console](#) and choosing **Copy S3 URI**.
6. Choose **Upload** to upload the manual evidence.

Note

When a control is in *inactive* status, you can't upload manual evidence for that control. To upload manual evidence, you must first change the control status to either *under review* or *reviewed*. For instructions on how to change a control status, see [Step 5: Mark a control as reviewed \(optional\) \(p. 42\)](#).

Step 4. Add a comment for a control (optional)

You can add comments for any controls that you review. These comments are visible to the audit owner. For example, you can leave a comment to provide a status update and confirm that you remediated any issues with that control.

To add a comment to a control

1. From the **Notifications** page, review the list of control sets that were delegated to you. Find the control set that you want to leave a comment for, and choose the name of the related assessment.
2. Choose the **Controls** tab, scroll down to the **Control sets** table, and then select the name of a control to open it.
3. Choose the **Comments** tab.
4. Under **Send comments**, enter your comment in the text box.
5. Choose **Submit comment** to add your comment. Your comment now appears under the **Previous comments** section of the page, along with any other comments regarding this control.

Step 5: Mark a control as reviewed (optional)

Changing the status of a control is optional. However, we recommend that you change the status of each control to **Reviewed** as you complete your review for that control. Regardless of the status of each individual control, you can still submit the controls to the audit owner.

To mark a control as reviewed

1. From the **Notifications** page, review the list of control sets that were delegated to you. Find the control set that contains the control that you want to mark as reviewed. Then, choose the name of the related assessment to open the assessment detail page.
2. Under the **Controls** tab of the assessment detail page, scroll down to the **Control sets** table.
3. Under the **Controls grouped by control set** column, expand the name of a control set to show its controls. Choose the name of a control to open the control detail page.
4. Choose **Update control status** and change the status to **Reviewed**.
5. In the pop-up window that appears, choose **Update control status** to confirm that you finished reviewing the control.

Step 6. Submit the reviewed control set back to the audit owner

When you're done reviewing all controls, submit the control set back to the audit owner to let them know you finished your review.

To submit a reviewed control set back to the owner

1. In the **Notifications** page, review the list of control sets that were assigned to you. Find the control set that you want to submit to the audit owner, and choose the name of the related assessment.

2. Scroll down to the **Control sets** table, select the control set that you want to submit back to the audit owner, and then choose **Submit for review**.
3. In the pop-up window that appears, you can add any high-level comments about that control set before choosing **Submit for review**.

After you submit the control to the audit owner, the audit owner can view any comments that you left for them.

Where do I go from here?

You can continue to learn more about the concepts that are introduced in this tutorial. The following are some recommended resources:

- [Reviewing an assessment \(p. 56\)](#) - Introduces you to the assessment page, where you can explore the different components of an assessment in AWS Audit Manager.
- [Review the controls in an assessment](#) and [Review the evidence in an assessment](#) - Provides data definitions to help you interpret the controls and evidence for each assessment.
- [AWS Audit Manager concepts and terminology \(p. 2\)](#) - Provides definitions for the concepts and terminology that are used in Audit Manager.

Using the Audit Manager dashboard

With the Audit Manager dashboard, you can visualize non-compliant evidence in your active assessments. It's a convenient and fast way to monitor your assessments, stay informed, and remediate issues proactively. By default, the dashboard provides a top-down, aggregated view of all your active assessments. Using this view, you can visually identify issues in your assessments without first needing to sift through vast amounts of individual evidence.

The dashboard is the first screen that you see when you sign in to the Audit Manager console. It contains two widgets that show the data and key performance indicators (KPIs) that are most relevant to you. Using an assessment filter, you can refine this data to focus on the KPIs for a specific assessment. From there, you can review control domain groupings to identify which controls have the most non-compliant evidence. Then, you can explore the underlying controls to examine and remediate issues.

Note

If you're a first-time Audit Manager user or you don't have any active assessments, no data is displayed in the dashboard. To get started, [create an assessment](#). This starts the ongoing collection of evidence. After a 24-hour period, aggregated evidence data will start to appear in the dashboard. You can read the following sections to learn how to understand and interpret this data.

This page covers the following topics:

Topics

- [Dashboard concepts and terminology \(p. 44\)](#)
- [Dashboard elements \(p. 46\)](#)
- [What do I do next? \(p. 49\)](#)
- [Troubleshooting \(p. 49\)](#)

Dashboard concepts and terminology

This section covers important things to know about the Audit Manager dashboard before you get started using it.

Permissions and visibility

Both [audit owners](#) and [delegates](#) have access to the dashboard. This means that both of these personas can see the metrics and aggregates for all active assessments in your AWS account. Having access to the same information enables all of your team to focus on the same KPIs and goals.

Filters

Audit Manager provides a page-level [the section called "Assessment filter" \(p. 46\)](#) that you can apply to all of the widgets on your dashboard.

Non-compliant evidence

The dashboard highlights the controls in your assessments that have [compliance check evidence](#) with a *non-compliant* conclusion. Compliance check evidence relates to controls that use AWS Config or AWS Security Hub as a data source type. For this evidence type, Audit Manager reports the result of a compliance check directly from those services. If Security Hub reports a *Fail* result, or if AWS Config reports a *Non-compliant* result, Audit Manager classes the evidence as non-compliant.

Inconclusive evidence

Evidence is *inconclusive* if a compliance check isn't available or applicable. As a result, no compliance evaluation can be made. This is the case if a control uses AWS Config or AWS Security Hub as a data source type but you didn't enable those services. This is also the case if the control uses a data source type that doesn't support compliance checks, such as manual evidence, AWS API calls, or AWS CloudTrail.

If evidence has a compliance check status of *not applicable* in the console, it's classified as *inconclusive* in the dashboard.

Compliant evidence

Evidence is *compliant* if a compliance check reported no issues. This is the case if Security Hub reports a *Pass* result, or AWS Config reports a *Compliant* result.

Control domains

The dashboard introduces the concept of a *control domain*. You can think of a control domain as a general category of controls that isn't specific to any one framework. Control domain groupings are one of the most powerful features of the dashboard. Audit Manager highlights the controls in your assessments that have non-compliant evidence, and groups them by control domain. Using this feature, you can focus your remediation efforts on specific subject domains as you prepare for an audit.

Note

A control domain is different to a *control set*. A control set is a framework-specific grouping of controls that's typically defined by a regulatory body. For example, the PCI DSS framework has a control set named *Requirement 8: Identify and authenticate access to system components*. This control set falls under the control domain of *Identity and access management*.

Audit Manager categorizes controls under the following control domains.

Control domain name	Description of what these controls govern
Business continuity and contingency planning	How you establish processes that protect critical business operations from the effects of major system and network disruptions.
Change management	How you test, approve, implement, and document changes to your cloud infrastructure.
Data security and privacy	How you secure the privacy, availability, and integrity of your data.
Development and configuration management	How you maintain your cloud infrastructure in a desired and consistent state.
Governance and oversight	How you align your use of cloud computing with your legal, regulatory, and ethical obligations.
Identity and access management	How you ensure that the right users have the appropriate access to your technology resources.
Incident management	How you establish responsibilities and procedures that ensure a quick and effective response to security incidents.
Logging and monitoring	How you review user activity for indications that unauthorized activity was attempted or performed.

Control domain name	Description of what these controls govern
Network management	How you administer and operate your data network using a network management system.
Personnel management	How you assess and manage personnel security risks at an organizational level.
Physical security	How you detect and prevent physical security issues in your facilities.
Risk management	How you evaluate potential risks and losses, and how you reduce or eliminate such threats.
Supply chain management	How you identify, assess, and mitigate the risks that are associated with IT products, vendors, and supply chains.
User device management	How you reduce the risk that your employees' IT hardware is lost, damaged, or compromised.
Vulnerability management	How you define, assess, and remediate all known vulnerabilities for assets within your cloud infrastructure.

Eventual consistency of data

The dashboard data is *eventually consistent*. This means that, when you read data from the dashboard, it might not instantly reflect the results of a recently completed write or update operation. If you check again within a few hours, the dashboard should reflect the latest data.

Data from deleted and inactive assessments

The dashboard displays data from active assessments. If you delete an assessment or change its status to inactive on the same day that you view the dashboard, data is included for that assessment as follows.

- **Inactive assessments** – If Audit Manager collected evidence for your assessment before you changed it to inactive, that evidence data is included in the dashboard counts for that day.
- **Deleted assessments** – If Audit Manager collected evidence for your assessment before you deleted it, that evidence data isn't included in the dashboard counts for that day.

Dashboard elements

The following sections cover the different components of the dashboard.

Topics

- [Assessment filter \(p. 46\)](#)
- [Daily snapshot \(p. 47\)](#)
- [Controls with non-compliant evidence grouped by control domain \(p. 47\)](#)

Assessment filter

You can use the assessment filter to focus on a specific active assessment.

By default, the dashboard displays aggregated data for all your active assessments. If you want to view data for a specific assessment, you apply an assessment filter. This is a page-level filter that applies to all widgets on the dashboard.

The screenshot shows the AWS Audit Manager Dashboard. At the top left is the title "Dashboard" with an "Info" link. Below it is the text "Last updated: October 29, 2021, 6:30 PM UTC". On the right side, there is a "Filter by" dropdown menu set to "All active assessments (7)" with a downward arrow, and a "Create assessment" button. A yellow box highlights the "Filter by" dropdown.

To apply the assessment filter, select an assessment from the drop-down list at the top of the dashboard. This list shows up to 10 of your active assessments. The most recently created assessments appear first. If you have many active assessments, you can start typing the name of an assessment to quickly find it. After you select an assessment, the dashboard displays data for that assessment only.

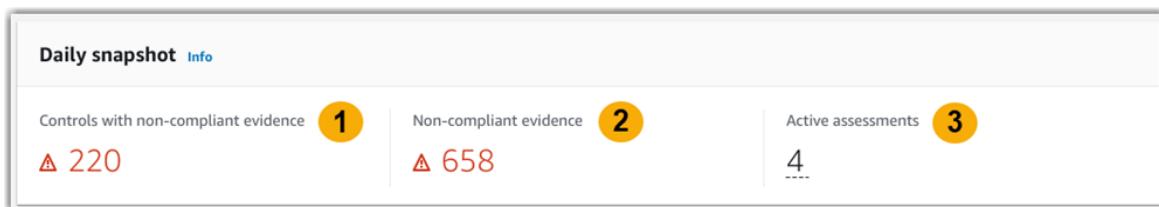
Daily snapshot

This widget shows a snapshot of the current compliance status of your active assessments.

The daily snapshot reflects the latest data that was collected on the date at the top of the dashboard. The date and time on the dashboard are represented in Coordinated Universal Time (UTC). It's important to understand that these numbers are daily counts based on this timestamp. They aren't a total sum to date.

By default, the daily snapshot shows the following data for all your active assessments:

- Controls with non-compliant evidence** - The total number of controls that are associated with non-compliant evidence.
- Non-compliant evidence** - The total amount of compliance check evidence with a *non-compliant* conclusion.
- Active assessments** - The total number of your active assessments. Choose this number to see links to these assessments.

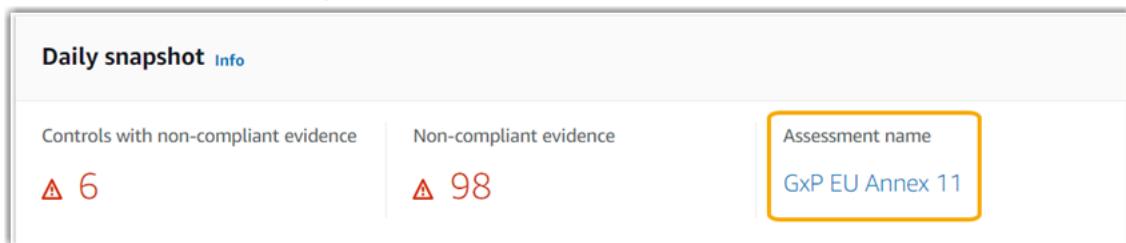


The screenshot shows the "Daily snapshot" section with three data points:

- Controls with non-compliant evidence: ▲ 220 (labeled 1)
- Non-compliant evidence: ▲ 658 (labeled 2)
- Active assessments: 3 (labeled 3)

Each data point has a red triangle icon indicating a change.

The daily snapshot data changes based on the [the section called "Assessment filter" \(p. 46\)](#) that you apply. When you specify an assessment, the data reflects the daily counts for that assessment only. In this case, the daily snapshot shows the name of the assessment that you specified. You can choose the name of the assessment to open it.



The screenshot shows the "Daily snapshot" section with three data points:

- Controls with non-compliant evidence: ▲ 6
- Non-compliant evidence: ▲ 98
- Assessment name: GxP EU Annex 11 (labeled 4)

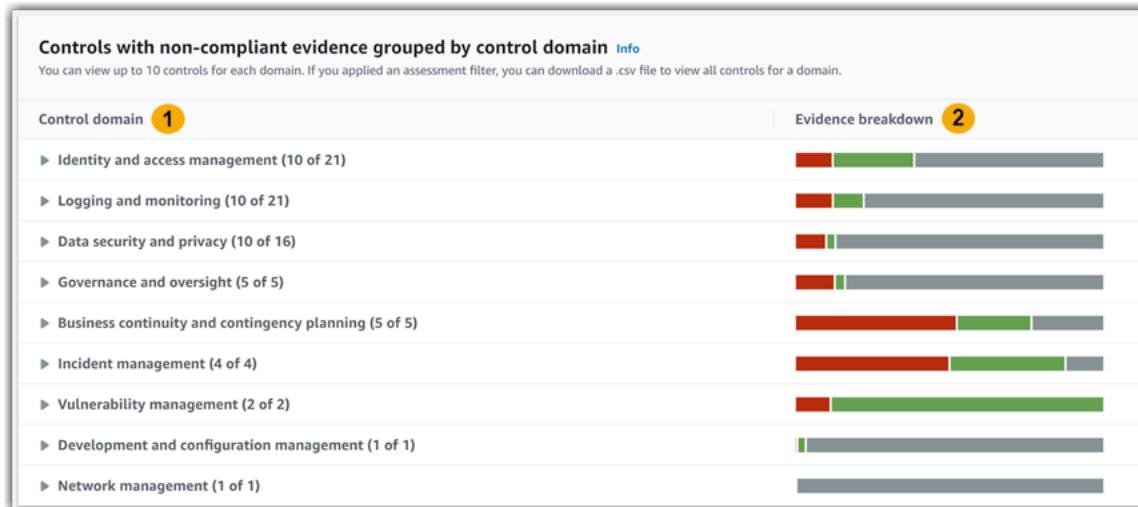
Each data point has a red triangle icon indicating a change. The "Assessment name" field is highlighted with a yellow box.

Controls with non-compliant evidence grouped by control domain

You can use this widget to identify which controls have the most non-compliant evidence.

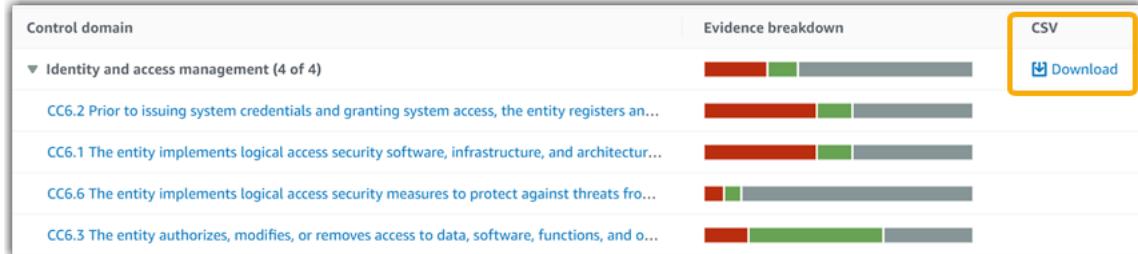
By default, the widget shows the following data for all your active assessments:

1. **Control domain** – A list of the [control domains \(p. 45\)](#) that are associated with your active assessments.
2. **Evidence breakdown** – A bar chart that shows a breakdown of the evidence compliance status.



To expand a control domain, choose the arrow next to its name. When expanded, the console shows up to 10 controls for each domain. These controls are ranked according to the highest total count of non-compliant evidence.

The data in this widget changes based on the [the section called “Assessment filter” \(p. 46\)](#) that you apply. When you specify an assessment, you see data for that assessment only. In addition, you can also download a .csv file for each available control domain in the assessment.



The .csv file includes the full list of controls in the domain that are associated with non-compliant evidence. The following example shows the .csv data columns with fictionalized values.

A	B	C	D	E	F	G
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	abcdefghijkl-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-defgijklmn	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-efgijklmnop	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-bcde-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-ghijklmnopq	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-bcde-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-ghi-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-efgh-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	fghijkl-6789-ghi-7890-hijklmnopqr	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-efgh-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-jklmnpqr	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						

Lastly, when you apply an assessment filter, the control names under each domain are hyperlinked. Choose any control to open the control details page in the specified assessment.



Tip

Using the control details page as your starting point, you can move from one level of detail to the next.

1. **Control details page** - On this page, the [evidence folders tab](#) lists daily folders of evidence that Audit Manager collected for that control. For more detail, choose a folder.
2. **Evidence folder** - Next, you can review a [folder summary](#) and a [list of the evidence](#) in that folder. For more detail, choose an individual evidence item.
3. **Individual evidence** - Lastly, you can explore [individual evidence details](#). This includes any applicable attributes and resource data for the evidence. This is the most granular level of evidence data.

What do I do next?

Here are some next steps that you can take after reviewing the dashboard.

- **Download a .csv file** – Find the assessment and control domain that you want to focus on, and [download the full list of related controls with non-compliant evidence](#).
- **Review a control** – After you identify a control that needs remediation, you can [review the control](#).
- **Delegate a control for review** – If you need assistance reviewing a control, you can [delegate a control set for review](#).
- **Edit your assessment** – If you want to change the scope of an active assessment, you can [edit the assessment](#).
- **Update the status of your assessment** – If you want to stop collecting evidence for an assessment, you can [change the assessment to inactive](#).

Troubleshooting

To find answers to common questions and issues, see [Troubleshooting dashboard issues](#) in the *Troubleshooting* section of this guide.

Assessments in AWS Audit Manager

An Audit Manager assessment is based on a framework, which is a grouping of controls. Using a framework as a starting point, you can create an assessment that collects evidence for the controls in that framework. In your assessment, you can also define the scope of your audit. This includes specifying the AWS accounts and services that you want to collect evidence for.

You can create an assessment from any framework. Either you can use a [standard framework](#) that's provided by Audit Manager. Or, you can create an assessment from a [custom framework](#) that you build yourself. Standard frameworks contain prebuilt control sets that support a specific compliance standard or regulation. In contrast, custom frameworks contain controls that you can customize and group according to your internal audit requirements. For more information about the differences between standard and custom frameworks, see [Frameworks](#) in the *Concepts and terminology* section of this guide.

When you create an assessment, this starts the ongoing collection of evidence. When it's time for an audit, you or a delegate can review this evidence and then add it to an assessment report.

Note

AWS Audit Manager assists in collecting evidence that's relevant for verifying compliance with specific compliance standards and regulations. However, it doesn't assess your compliance itself. The evidence that's collected through AWS Audit Manager therefore might not include all the information about your AWS usage that's needed for audits. AWS Audit Manager isn't a substitute for legal counsel or compliance experts.

Topics

- [Creating an assessment \(p. 50\)](#)
- [Accessing your assessments in AWS Audit Manager \(p. 54\)](#)
- [Editing an assessment \(p. 54\)](#)
- [Reviewing an assessment \(p. 56\)](#)
- [Reviewing the controls in an assessment \(p. 60\)](#)
- [Reviewing the evidence in an assessment \(p. 63\)](#)
- [Adding manual evidence in AWS Audit Manager \(p. 67\)](#)
- [Generating an assessment report \(p. 73\)](#)
- [Changing the status of an assessment to inactive \(p. 76\)](#)
- [Deleting an assessment \(p. 77\)](#)

Creating an assessment

This topic builds on the [Getting started: Creating an assessment](#) tutorial. It contains detailed instructions on how to create an assessment from a framework. Follow these steps to create an assessment and start the ongoing collection of evidence.

Tasks

- [Step 1: Specify assessment details \(p. 51\)](#)
- [Step 2: Specify AWS accounts in scope \(p. 51\)](#)
- [Step 3: Specify AWS services in scope \(p. 52\)](#)
- [Step 4: Specify audit owners \(p. 53\)](#)
- [Step 5: Review and create \(p. 53\)](#)

- [What can I do next? \(p. 53\)](#)

Step 1: Specify assessment details

Start by selecting a framework and providing basic information for your assessment.

To specify assessment details

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Assessments**, and then choose **Create assessment**.
 - Alternatively, in the navigation pane, choose **Getting started**, and then choose **Create assessment**.
3. Under **Assessment name**, enter a name for your assessment.
4. (Optional) Under **Assessment description**, enter a description for your assessment.
5. Under **Assessment reports destination**, select an existing Amazon S3 bucket where you intend to save your assessment reports.

Tip

The default assessment report destination is based on your Audit Manager settings. For more information, see [AWS Audit Manager settings, Assessment report destination](#). If you prefer, you can create and use multiple S3 buckets to help you organize your assessment reports.

6. Under **Frameworks**, select the framework that you want to create your assessment from. You can also use the search bar to look up a framework by name, or by compliance standard or regulation.

Tip

To learn more about a framework, choose the framework name. This opens the framework summary page. On this page, you can review the contents of that framework. This includes the controls and data sources of the framework.

7. Under **Tags**, choose **Add new tag** to associate a tag with your assessment. You can specify a key and a value for each tag. The tag key is mandatory and can be used as a search criteria when you search for this assessment. For more information about tags in Audit Manager, see [Tagging AWS Audit Manager resources \(p. 367\)](#).
8. Choose **Next**.

Note

It's important to make sure that your assessment collects the correct evidence for a given framework. Before you begin evidence collection, we recommend that you review the requirements for your chosen framework. Then, validate these requirements against your current AWS Config rule parameters. To ensure that your rule parameters align with framework requirements, you can [update the rule in AWS Config](#).

For example, suppose that you're creating an assessment for CIS v1.2.0. This framework has a control named [1.9 – Ensure IAM password policy requires a minimum length of 14 or greater](#). In AWS Config, the [iam-password-policy](#) rule has a MinimumPasswordLength parameter that checks password length. The default value for this parameter is 14 characters. As a result, the rule aligns with the control requirements. If you aren't using the default parameter value, ensure that the value you're using is equal to or greater than the 14 character requirement from CIS v1.2.0. You can find the default parameter details for each managed rule in the [AWS Config documentation](#).

Step 2: Specify AWS accounts in scope

You can specify multiple AWS accounts to be in the scope of an assessment. Audit Manager supports multiple accounts through integration with AWS Organizations. This means that Audit Manager

assessments can be run over multiple accounts, with the evidence that's collected consolidated into a delegated administrator account. To enable Organizations in Audit Manager, see [Enable AWS Organizations \(optional\) \(p. 34\)](#).

Note

Audit Manager can support up to approximately 150 accounts in the scope of an assessment. If you try to include over 150 accounts, the assessment creation might fail.

To specify AWS accounts in scope

1. Under **AWS accounts**, select the AWS accounts that you want to include in the scope of your assessment.
 - If you enabled Organizations in Audit Manager, multiple accounts are displayed. You can choose one or more accounts from the list. Alternatively, you can also search for an account by the account name, ID, or email.
 - If you didn't enable Organizations in Audit Manager, only your current AWS account is listed.
2. Choose **Next**.

Note

When an in-scope account is removed from your organization, Audit Manager no longer collects evidence for that account. However, the account continues to show in your assessment under the **AWS accounts** tab. To remove the account from the list of accounts in scope, you can [edit the assessment](#). The removed account no longer shows in the list during editing, and you can save your changes without that account in scope.

Step 3: Specify AWS services in scope

The framework that you selected earlier defines the AWS services that Audit Manager monitors and collects evidence for. If a listed AWS service isn't selected, or it's selected but you didn't enable it in your environment, then Audit Manager doesn't collect evidence from resources related to that service.

You can specify the AWS services in scope as follows.

For assessments created from standard frameworks

When you use the Audit Manager console to create an assessment from a standard framework, the list of AWS services in scope is selected by default. This list can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the standard framework. If the standard framework that you selected contains only manual controls, no AWS services are in scope for your assessment, and you can't add any services to your assessment.

To proceed, review the list and choose **Next**.

Tip

If you need to edit the list of services in scope, you can do so by using the [CreateAssessment](#) API that's provided by Audit Manager.

Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For assessments created from custom frameworks

If you selected a custom framework in [step 1](#), you can review and modify the list of AWS services that are in scope for your assessment. If the custom framework that you selected contains manual controls only, all AWS services are displayed but none are selected. You can select zero or more services to be in the scope of your assessment.

To specify AWS services in scope (for assessments created from custom frameworks only)

1. Under **AWS services**, select the services that you want to include in your assessment. You can find additional services by using the search bar to search by service, category, or description. To add a service, select the check box next to the service name. To remove a service, clear the check box.
2. When you're finished selecting AWS services, choose **Next**.

Step 4: Specify audit owners

In this step, you specify the audit owners for your assessment. Audit owners are the individuals in your workplace—usually from GRC, SecOps, or DevOps teams—who are responsible for managing the Audit Manager assessment. We recommend that they use the [AWSAuditManagerAdministratorAccess](#) policy.

To specify audit owners

1. Under **Audit owners**, review the current list of audit owners. The **Audit owner** column displays the user IDs and roles. The **AWS account** column displays the associated AWS account of that audit owner.
2. Audit owners that have a selected check box are included in your assessment. Clear the check box for any audit owner to remove them from the assessment. You can find additional audit owners by using the search bar to search by name or AWS account.
3. When you're finished, choose **Next**.

Step 5: Review and create

Review the information for your assessment. To change the information for a step, choose **Edit**. When you're finished, choose **Create assessment**.

This action starts the ongoing collection of evidence for your assessment. After you create an assessment, evidence collection continues until you [change the assessment status](#) to *inactive*. Alternatively, you can stop evidence collection for a specific control by [changing the control status](#) to *inactive*.

Note

Automated evidence becomes available 24 hours after your assessment's created. Audit Manager automatically collects evidence from multiple data sources, and the frequency of that evidence collection is based on the evidence type. To learn more, see [Evidence collection frequency \(p. 12\)](#) in this guide.

What can I do next?

After you create your assessment, you can learn more about the following:

- [Accessing an assessment](#)
- [Reviewing an assessment \(p. 56\)](#)
- [Editing an assessment \(p. 54\)](#)
- [Reviewing the controls in an assessment \(p. 60\)](#)
- [Reviewing the evidence in an assessment \(p. 63\)](#)
- [Uploading manual evidence to an assessment](#)
- [Delegations in AWS Audit Manager \(p. 79\)](#)
- [Generating an assessment report \(p. 73\)](#)

- [Changing the status of an assessment](#)
- [Deleting an assessment \(p. 77\)](#)
- [Troubleshooting assessment and evidence collection issues \(p. 272\)](#)

Accessing your assessments in AWS Audit Manager

You can view all of your assessments on the **Assessments** page in the Audit Manager console. From here, you can also [edit an assessment](#), [delete an assessment](#), or [create an assessment](#).

You can also view your assessments using the Audit Manager API or the AWS Command Line Interface (AWS CLI).

Audit Manager console

To view your assessments (console)

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the left navigation pane, choose **Assessments** to see a list of your active and past assessments. You can also use the search bar to search for an assessment.
3. Choose any assessment name to open a summary page, where you can view the details for that assessment.

AWS CLI

To view your assessments (CLI)

To view assessments in Audit Manager, run the [list-assessments](#) command. You can use the --status subcommand to view assessments that are active or inactive.

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

```
aws auditmanager list-assessments --status INACTIVE
```

Audit Manager API

To view your assessments (API)

To view assessments in Audit Manager, use the [ListAssessments](#) operation. You can use the [status](#) attribute to view assessments that are active or inactive.

For more information, choose either of the previous links to read more in the *AWS Audit Manager API Reference*. This includes information about how to use the ListAssessments operation and parameters in one of the language-specific AWS SDKs.

Editing an assessment

You can edit your active assessments in Audit Manager to change information such as the description, scope, audit owners, and assessment report destination.

Tasks

- [Step 1: Edit assessment details \(p. 55\)](#)
- [Step 2: Edit AWS accounts in scope \(p. 55\)](#)
- [Step 3: Edit AWS services in scope \(p. 55\)](#)
- [Step 4: Edit audit owners \(p. 56\)](#)
- [Step 5: Review and save \(p. 56\)](#)

Step 1: Edit assessment details

Follow these steps to edit the details of your assessment.

To edit an assessment

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Assessments** to view your current list of assessments.
3. Select an assessment, and choose **Edit**.
 - Alternatively, you can open the assessment and then choose **Edit** in the top right of the page.
4. Under **Edit assessment details**, edit your assessment name, description, and assessment report destination.
5. Choose **Next**.

Tip

To edit the tags for an assessment, open the assessment and choose the [Tags tab \(p. 60\)](#). There you can view and edit the tags associated with the assessment.

Step 2: Edit AWS accounts in scope

In this step, you can change the list of accounts that are included in the scope of your assessment.

Audit Manager supports multiple accounts through integration with AWS Organizations. This means that Audit Manager assessments can be run over multiple accounts, with the collected evidence consolidated into a delegated administrator account. To add or change the delegated administrator for Audit Manager, see [AWS Audit Manager settings, Delegated administrator](#).

Note

Audit Manager can support up to approximately 150 accounts in the scope of an assessment. If you try to include over 150 accounts, the assessment creation might fail.

To edit AWS accounts in scope

1. Under **Edit AWS accounts in scope**, select additional AWS accounts. You can also remove accounts by clearing them from the list.
2. Choose **Next**.

Step 3: Edit AWS services in scope

This step specifies which AWS services Audit Manager monitors and collects evidence for. If a listed AWS service isn't selected, or it's selected but you didn't enable it in your environment, Audit Manager doesn't collect evidence from resources related to that service.

You can review and edit the AWS services in scope as follows.

For assessments created from standard frameworks

When you use the Audit Manager console to edit an assessment that was created from a standard framework, you can review the list of AWS services in scope but you can't edit this list. This is because Audit Manager automatically maps and selects the data sources and services for you, according to the design of the standard framework. If the assessment was created using a framework that contains manual controls only, no AWS services are in scope for your assessment, and you can't add any services.

To proceed, review the list and choose **Next**.

Tip

If you need to edit the list of services in scope for an existing assessment, you can do so by using the [UpdateAssessment](#) API that's provided by Audit Manager.

For assessments created from custom frameworks

If you created the assessment from a custom framework, you can edit the AWS services that are in scope for your assessment. You can select zero or more services to be in the scope of your assessment.

To edit AWS services in scope (for assessments created from custom frameworks only)

1. Under **Edit AWS services in scope**, select additional AWS services as necessary. You can also remove services by clearing them from the list.
2. Choose **Next**.

Step 4: Edit audit owners

You can also change the audit owners for your assessment. Audit owners are the individuals in your workplace—usually from GRC, SecOps, or DevOps teams—who are responsible for managing the Audit Manager assessment. Their duties include delegating control sets for review and generating assessment reports. We recommend that you use the [AWSAuditManagerAdministratorAccess](#) policy.

To edit audit owners

1. Select new audit owners to add to the assessment. To remove audit owners, clear them from the list.
2. Choose **Next**.

Step 5: Review and save

Review the information for your assessment. To change the information for a step, choose **Edit**. When you're finished, choose **Save changes** to confirm your edits.

Note

After you complete your edits, the changes to the assessment take effect at 00:00 UTC the following day.

Reviewing an assessment

After you create assessments in Audit Manager, you can open and review your assessments at any time.

To open and review an assessment

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.

2. In the left navigation pane, choose **Assessments** to see a list of your assessments.
3. Choose the name of the assessment to open it.

When you open an assessment, you see a summary page that contains several sections. The sections of this page and their contents are described as follows.

Sections of the assessment page

- [Assessment details \(p. 57\)](#)
- [Controls tab \(p. 58\)](#)
- [Assessment report selection tab \(p. 58\)](#)
- [AWS accounts tab \(p. 59\)](#)
- [AWS services tab \(p. 59\)](#)
- [Audit owners tab \(p. 59\)](#)
- [Tags tab \(p. 60\)](#)
- [Changelog tab \(p. 60\)](#)

Assessment details

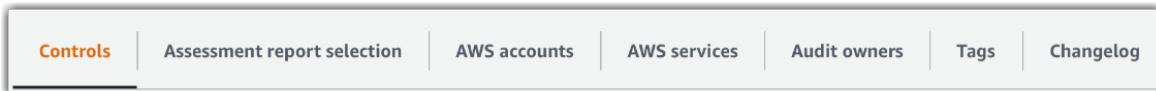
The **Assessment details** section provides an overview of the assessment.

Assessment details	
Name	1 FedRampAssessment
Description	2 -
Compliance type	3 FedRAMP
Assessment report selection	4 0
Total evidence	5 0
Assessment reports destination	6 s3://
AWS accounts	7 1
AWS services	8 11
Audit owners	9 1
Assessment status	10 Active
Date created	11 November 21, 2020, 1:16 AM UTC
Last updated	12 November 21, 2020, 1:17 AM UTC

It includes the following information:

1. **Name** – The name that you provided for the assessment.
2. **Description** – The optional description that you provided for the assessment.
3. **Compliance type** – The compliance standard or regulation that the assessment supports.
4. **Assessment report selection** – The number of evidence items that you choose to include in the assessment report.
5. **Total evidence** – The total number of evidence items that are collected for this assessment.
6. **Assessment reports destination** – The Amazon S3 bucket that Audit Manager saves the assessment report in.
7. **AWS accounts** – The number of AWS accounts that are in scope for this assessment.
8. **AWS services** – The number of AWS services that are in scope for this assessment.
9. **Audit owners** – The number of audit owners for this assessment.
- 10 **Assessment status** – The status of the assessment.
 - **Active** - Indicates that the assessment is currently collecting evidence. Newly created assessments have this status.
 - **Inactive** - Indicates that the assessment is no longer collecting evidence. For more information about inactive assessments, see [Changing the status of an assessment to inactive \(p. 76\)](#).
- 11 **Date created** – The date that the assessment was created.
- 12 **Last updated** – The date when this assessment was last edited.

Controls tab



The **Controls** tab displays a summary of the controls in the assessment, along with a full list of those controls. Each assessment can contain multiple control sets, and each control set contains multiple controls. Controls and control sets are organized so that they match the layout defined in the associated compliance standard or regulation.

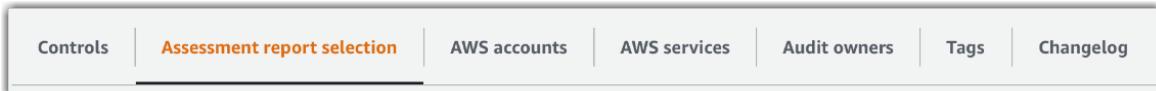
Under **Control status summary**, you can review a summary of the controls for this assessment. The summary includes the following information:

- **Total controls** – The total number of controls in this assessment.
- **Reviewed** – The number of controls that were reviewed by an audit owner or delegate.
- **Under review** – The number of controls that are currently under review.
- **Inactive** – The number of controls that are no longer actively collecting evidence.

Under the **Control sets** table, a list of controls is displayed and grouped by control set. You can expand or collapse the controls in each control set. You can also search by control name if you want to look for a particular control. The following data columns appear in the **Controls grouped by control sets** table:

- **Controls grouped by control sets** – The name of the control set.
- **Control status** – The status of the control.
 - **Under review** indicates that this control isn't already reviewed. Evidence is still being collected for this control, and you can upload manual evidence. This is the default status.
 - **Reviewed** indicates that the evidence for this control was reviewed. However, evidence is still being collected, and you can upload manual evidence.
 - **Inactive** indicates automated evidence collection is stopped for this control. You can no longer upload manual evidence.
- **Delegated to** – The reviewer of this control, if it was assigned to a delegate for review.
- **Total evidence** – The number of evidence items that have been collected for this control.

Assessment report selection tab



This tab displays the list of evidence to be included in the assessment report, grouped by evidence folders. These evidence folders are organized and named based on the date when they were created. You can browse these folders and select which evidence you want to include in your assessment report. You can also use the search bar to search by evidence folder name or control name. The total number of evidence items that are added to the assessment report is summarized under the **Assessment details** section at the top of the page.

The **Assessment report selection** table shows a list of evidence folders with the following data:

- **Evidence folder** – The name of the evidence folder. The folder name is based on the date when the evidence was collected.
- **Selected evidence** – The number of evidence items within the folder that are included in the assessment report.

- **Control name** – The name of the control that's associated with this evidence folder.

For information about adding evidence to an assessment report, see [Generating an assessment report \(p. 73\)](#).

AWS accounts tab



This tab displays the list of AWS accounts that are in the scope of the assessment. The total number of accounts is summarized under the **Assessment details** section at the top of the page.

The **AWS accounts** table shows a list of accounts with the following data:

- **Account ID** – The ID of the AWS account.
- **Account name** – The name of the AWS account.
- **Email** – The email address that's associated with the AWS account.

AWS services tab



This tab displays the list of AWS services that are in the scope of the assessment. In other words, these are the AWS services that your assessment collects evidence about.

The total number of services is summarized under the **Assessment details** section at the top of the page.

The **AWS services** table shows a list of services with the following data:

- **AWS service** – The name of the AWS service.
- **Category** – The service category, such as *compute* or *database*.

Audit Manager performs resource assessments for the services in this table. For example, if Amazon S3 is listed, Audit Manager can collect evidence about your S3 buckets. The exact evidence that's collected is determined by a control's [data source](#). For instance, if the data source type is AWS Config, and the data source mapping is an AWS Config rule (such as `s3-bucket-public-write-prohibited`), Audit Manager collects the result of that rule evaluation as evidence. For more information, see [What's the difference between a service in scope and a data source type?](#) in this guide.

Note

If your assessment was created in the console from a standard framework, Audit Manager selected the services for you and mapped their data sources according to the framework's requirements. If the standard framework contains only manual controls, no AWS services are in scope. If you need to edit the list of services in scope, you can use the [UpdateAssessment API](#).

Audit owners tab



This tab displays the audit owners for the assessment. The total number of audit owners is also summarized under the **Assessment details** section at the top of the page.

The **Audit owners** table shows a list of accounts with the following data:

- **Audit owner** – The name of the audit owner.
- **AWS account** – The email address that's associated with the audit owner.

Tags tab



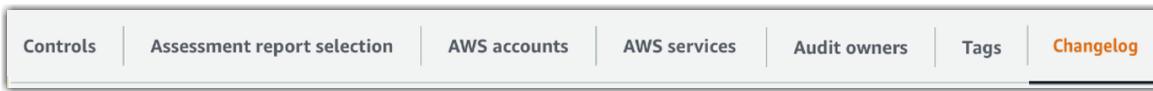
This tab displays the list of tags inherited from the framework are used to create this assessment. The total number of tags is summarized under **Assessment detail** at the top of the page.

The **Tags** table shows a list of tags with the following data:

- **Key** - The key of the tag, such as a compliance standard, regulation, or category.
- **Value** - The value of the tag.

For more information about tags in Audit Manager, see [Tagging AWS Audit Manager resources \(p. 367\)](#).

Changelog tab



This tab displays a list of user activity related to the assessment.

The **Changelog** table shows a list of accounts with the following data:

- **Date** – The date of the activity.
- **User** – The user who performed the action.
- **Action** – The action that occurred, such as an assessment being created.
- **Type** – The object type that changed, such as an assessment.
- **Resource** – The resource that was affected by the change, such as the framework that the assessment was created from.

Reviewing the controls in an assessment

Controls in Audit Manager help you meet both common and unique compliance standards and regulations in your audits. You can open and review the controls in your Audit Manager assessment at any time.

To open a control summary page

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Assessments**, and choose the name of an assessment to open it.
3. From the assessment page, choose the **Controls** tab, scroll down to the **Control sets** table, and then choose the name of a control to open it.

When you open a control, you see a summary page that contains several sections. The sections of this page and their contents are described in the following sections.

Sections of the control page

- [Control details \(p. 61\)](#)
- [Update control status \(p. 61\)](#)
- [Evidence folders tab \(p. 61\)](#)
- [Data source tab \(p. 62\)](#)
- [Comments tab \(p. 62\)](#)
- [Changelog tab \(p. 63\)](#)

Control details

The **Control details** section provides an overview of the control.

It includes the following information:

1. **Control name** – The name that's given to this control.
2. **Control description** – The description that's provided for this control.
3. **Testing information** – The recommended testing procedures for this control.
4. **Action plan** – The recommended actions to carry out if the control isn't fulfilled.

Update control status

In the **Update control status** section of the page, you can review and update the status of the assessment control.

The following statuses are available:

- **Under review** – Indicates that this control hasn't been reviewed yet. Evidence is still being collected for this control, and you can upload manual evidence. This is the default status.
- **Reviewed** – Indicates that the evidence for this control is reviewed. Evidence is still being collected, and you can upload manual evidence.
- **Inactive** – Indicates that automated evidence collection is stopped for this control. You can no longer upload manual evidence.

Note

Changing a control status to *Reviewed* is final. After you set the status of a control to *Reviewed*, you can no longer change the status of that control or revert to a previous status.

Evidence folders tab

The **Evidence folders** tab lists the evidence that's automatically collected for this control. It's organized into folders on a daily basis.

The **Evidence folders** table shows a list of folders with the following data:

- **Evidence folder** – The name of the evidence folder. The name is based on the date when the evidence was collected or manually added.

- **Compliance check** – The number of issues that are found in the evidence folder. This number represents the total number of security issues that were reported directly from AWS Security Hub, AWS Config, or both. If you see **Not applicable**, this indicates that you either don't have AWS Security Hub or AWS Config enabled, or the evidence comes from a different data source type.
- **Total evidence** – The total number of evidence items inside the folder.
- **Assessment report selection** – The number of evidence items within the folder that are included in the assessment report.

From the **Evidence folders** tab, you can take the following actions:

- **Review individual evidence** – Choose an [evidence folder](#) to open it. From the evidence folder summary page, you can then choose the [individual evidence](#) that you want to review.
- **Add manual evidence** – For more information, see [Adding manual evidence in AWS Audit Manager \(p. 67\)](#).
- **Add evidence to an assessment report** – For more information, see [Generating an assessment report \(p. 73\)](#).

Data source tab

This tab displays information about the data sources for the control. It includes the following information:

- **Data source name** – This applies to custom controls only. It refers to the descriptive name that you gave each data source. You can use this name to distinguish between multiple data sources that fall under the same data source type
- **Data source type** – This specifies where the evidence data comes from.
 - If Audit Manager collects the evidence, the data source can be one of four types: *AWS Security Hub*, *AWS Config*, *AWS CloudTrail*, or *AWS API calls*.
 - If you upload your own evidence, the data source type is *Manual*. A description indicates if the required manual evidence is a *File upload* or a *Text response*.
- **Mapping** – This is the mapping attribute that's used to identify and retrieve data from an automated data source.
 - If the data source type is *AWS Config*, the mapping is the name of a specific AWS Config rule (for example, `EC2_INSTANCE_MANAGED_BY_SSM`). Audit Manager uses this mapping to report the result of that rule check directly from AWS Config.
 - If the data source type is *AWS Security Hub*, the mapping is the name of a specific Security Hub control (for example, `1.1 - Avoid the use of the "root" account`). Audit Manager uses this mapping to report the result of that security check directly from Security Hub.
 - If the data source type is *AWS API calls*, the mapping is the name of a specific API call (for example, `ec2_DescribeSecurityGroups`). Audit Manager uses this mapping to collect the API response.
 - If the data source type is *AWS CloudTrail*, the mapping is the name of a specific CloudTrail event (for example, `CreateAccessKey`). Audit Manager uses this mapping to collect the related user activity from your CloudTrail logs.
- **Frequency** – The frequency of evidence collection from this data source. The frequency varies depending on the data source. For more information, choose the value in the column or see [Evidence collection frequency \(p. 12\)](#).

Comments tab

In the **Comments** tab, you can add a comment regarding the control and its evidence. It also displays a list of previous comments.

Under **Send comments**, you can add comments for a control by entering text and then choosing **Submit comments**.

Under **Previous comments**, you can view a list of previous comments along with the date the comment was made and the associated user ID.

Changelog tab

The **Changelog** tab displays a list of user activity related to the control. The same information is available as audit trail logs in AWS CloudTrail. With the user activity that's captured directly in Audit Manager, you can easily review an audit trail of activity for a given control.

Under **Changelog**, a table displays the following data columns:

- **Date** – The date and time of the activity, represented in Coordinated Universal Time (UTC).
- **User** – The user or role that performed the activity.
- **Action** – A description of the activity.
- **Type** – The associated attribute that further describes the activity.
- **Resource** – The related resource, if applicable.

Audit Manager tracks the following user activity in changelogs:

- Creating an assessment
- Editing an assessment
- Completing an assessment
- Deleting an assessment
- Delegating a control set for review
- Submitting a reviewed control set back to the audit owner
- Uploading manual evidence
- Updating a control status
- Generating assessment reports

Reviewing the evidence in an assessment

An active assessment in Audit Manager automatically collects evidence from a range of data sources. For more information, see [How AWS Audit Manager collects evidence \(p. 11\)](#). You can open and review the evidence for the controls in your assessments at any time.

To open evidence for a control

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Assessments**, and then choose the name of an assessment to open it.
3. From the assessment page, choose the **Controls** tab, scroll down to the **Controls** table, and then choose the name of a control to open it.
4. From the control page, choose the **Evidence folders** tab. Under the **Evidence folders** table, a list of all evidence folders for that control is displayed. These folders are organized and named based on the date when the evidence within the folder was collected.
5. Choose the name of an evidence folder to open it.

From here, you can now review the evidence folders for that control, and drill down further to review individual pieces of evidence as needed.

Topics

- [Reviewing evidence folders \(p. 64\)](#)
- [Reviewing individual evidence \(p. 65\)](#)

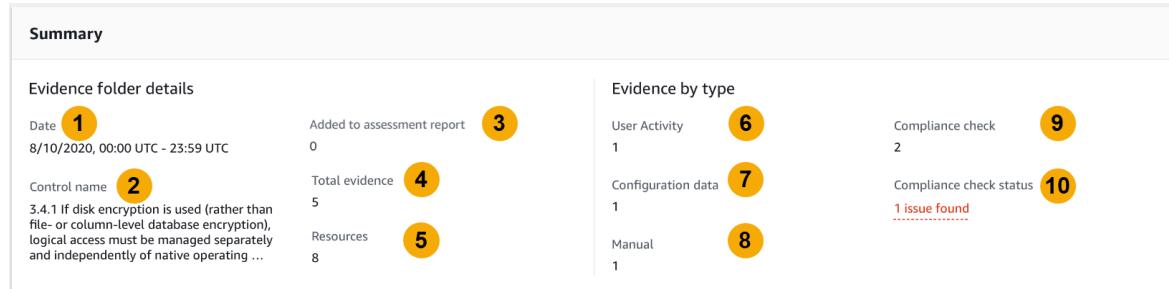
Reviewing evidence folders

When you open an evidence folder, you see an evidence folder summary page that contains two sections: a **Summary** section and an **Evidence** table. These sections and their contents are described as follows.

- [Evidence folder summary \(p. 64\)](#)
- [Evidence table \(p. 65\)](#)

Evidence folder summary

The **Summary** section of the page provides a high-level overview of the evidence in the evidence folder.



It includes the following information:

1. **Date** – The time and date when the evidence folder was created, represented in Coordinated Universal Time (UTC).
2. **Control name** – The name of the control that's associated with the evidence folder.
3. **Added to assessment report** – The number of evidence items that were manually selected for inclusion in the assessment report.
4. **Total evidence** – The total number of evidence items in the evidence folder.
5. **Resources** – The total number of AWS resources that were assessed when generating the evidence in this folder.
6. **User activity** – The number of evidence items that fall under the *user activity* category. This evidence is collected from AWS CloudTrail logs.
7. **Configuration data** – The number of evidence items that fall under the *configuration data* category. This evidence is collected from configuration snapshots of other AWS services such as Amazon EC2, Amazon S3, or IAM.
8. **Manual** – The number of evidence items that fall under the *manual* category. This evidence is uploaded manually.
9. **Compliance check** – The number of evidence items that fall under the *compliance check* category. This evidence is collected from AWS Config or AWS Security Hub.
10. **Compliance check status** – The total number of issues that were reported directly from AWS Security Hub, AWS Config, or both.

Tip

For more information about different evidence types (user activity, configuration data, compliance check, and manual), see [Evidence](#).

Evidence table

The **Evidence** table lists the individual pieces of evidence that are contained within the evidence folder.

It includes the following information:

1. **Time** – Specifies when the evidence was collected, and also serves as the name of the evidence. The time is represented in Coordinated Universal Time (UTC). Choosing a time from this column opens an [evidence detail page](#). This page is described in the following section.
2. **Evidence by type** – The category of the evidence.
 - **Compliance check** evidence is collected from AWS Config or AWS Security Hub.
 - **User activity** evidence is collected from AWS CloudTrail logs.
 - **Configuration data** evidence is collected from snapshots of other services such as Amazon EC2, Amazon S3, or IAM.
 - **Manual** evidence is evidence that you upload manually.
3. **Compliance check** – The evaluation status for evidence that falls under the *compliance check* category.
 - For evidence that's collected from AWS Security Hub, a **Pass** or **Fail** result is reported directly from AWS Security Hub.
 - For evidence that's collected from AWS Config, a **Compliant** or **Noncompliant** result is reported directly from AWS Config.
 - If **Not applicable** is shown, this indicates that you either don't have AWS Security Hub or AWS Config enabled, or the evidence comes from a different data source type.
4. **Data source** – The data source where the evidence is collected from.
5. **Event name** – The name of the event included in the evidence.
6. **Resources** – The number of resources assessed to generate the evidence.
7. **Assessment report selection** – Indicates whether that evidence was manually selected for inclusion in the assessment report.
 - To include evidence, select the evidence and choose **Add to assessment report**.
 - To exclude evidence, select the evidence and choose **Remove from assessment report**.

To upload manual evidence to the evidence folder, choose **Upload manual evidence**, enter the S3 URI of the evidence, and then choose **Upload**. For more information, see [Uploading manual evidence in AWS Audit Manager](#).

To see details for any individual piece of evidence, choose the hyperlinked evidence name under the **Time** column. This opens an evidence detail page, which is described in the following section.

Reviewing individual evidence

When you open an individual piece of evidence, you see an evidence detail page that contains three sections: the **Evidence detail** section, the **Attributes** table, and the **Resources included** table. These sections and their contents are described as follows.

- [Evidence detail \(p. 66\)](#)
- [Attributes \(p. 66\)](#)
- [Resources included \(p. 67\)](#)

Evidence detail

The **Evidence detail** section of the page displays an overview of the evidence.

Evidence detail			
Date and time 1 8/10/20, 18:55:18 UTC	Event source 4 iam.amazonaws.com	Evidence by type 7 User activity	AWS account 11 Account name (# [REDACTED])
Evidence folder name 2 2020-08-10	Event name 5 UpdateAccountPasswordPolicy	Compliance check 8 Not applicable	IAM ID 12 [REDACTED]
Control name 3 Ensure IAM password policy requires minimum password length of 20 or greater	Data source 6 AWS CloudTrail	Resources included 9 2	Added to assessment report 13 No
		Attributes 10 4	

It includes the following information:

1. **Date and time** – The date and time when the evidence was collected, represented in Coordinated Universal Time (UTC).
2. **Evidence folder name** – The name of the evidence folder that contains the evidence.
3. **Control name** – The name of the control that's associated with the evidence.
4. **Event source** – The name of the resource that created the evidence event.
5. **Event name** – The name of the evidence event.
6. **Data source** – The data source where the evidence was collected from.
7. **Evidence by type** – The type of evidence.
 - **Compliance check** evidence is collected from AWS Config or AWS Security Hub.
 - **User activity** evidence is collected from AWS CloudTrail logs.
 - **Configuration data** evidence is collected from snapshots of other AWS services such as Amazon EC2, Amazon S3, or IAM.
 - **Manual** evidence is evidence that you upload manually.
8. **Compliance check** – The evaluation status for evidence that falls under the *compliance check* category.
 - For evidence that's collected from AWS Security Hub, a **Pass** or **Fail** result is reported directly from AWS Security Hub.
 - For evidence that's collected from AWS Config, a **Compliant** or **Noncompliant** result is reported directly from AWS Config.
 - If **Not applicable** is shown, this indicates that you either don't have AWS Security Hub or AWS Config enabled, or the evidence comes from a different data source.
9. **Resources included** – The number of resources that are assessed to generate the evidence.
10. **Attributes** – The total number of attributes that are used by the event in the evidence.
11. **AWS account** – The AWS account where the evidence was collected from.
12. **IAM ID** – The relevant user or role, if applicable.
13. **Added to assessment report** – Indicates if you chose to include the evidence in the assessment report.

Attributes

The **Attributes** table displays the names and values that are used by the event in this evidence. It includes the following information:

- **Attribute name** – The requirement for the evidence, such as *allowUsersToChangePassword*.

- **Value** – The value of the attribute, such as *true* or *false*.

Resources included

The **Resources included** table displays the list of resources assessed to generate this evidence. It includes one or more of the following fields:

- **ARN** – The Amazon Resource Name (ARN) of the resource. An ARN might not be available for all evidence types.
- **Value** – The value of that resource, if applicable.
- **JSON** – The link to view the JSON file for that resource.

Adding manual evidence in AWS Audit Manager

Audit Manager can automatically collect evidence for many controls. However, some controls require you to manually add your own evidence.

Consider the following examples:

- Some controls relate to the provision of physical records (such as signatures), or events that aren't generated in the cloud (such as observations and interviews). In these cases, you can manually upload files as evidence. For instance, if a control requires information about your organizational structure, you can upload a copy of your company's org chart as manual evidence.
- Some controls represent a vendor risk assessment question. A risk assessment question might require documentation as evidence (such as an org chart). Or, it might only need a simple text response (such as a list of job titles). In the case of the latter, you can respond to the question and save your response as manual evidence.

You can also use the manual upload feature to manage evidence from multiple environments. If your company uses a hybrid cloud model or multicloud model, you can upload evidence from your on-premises environment, an environment hosted in the cloud, or your SaaS applications. This enables you to organize your evidence (regardless of where it came from) by storing it within the structure of an Audit Manager assessment, where each piece of evidence is mapped to a specific control.

To learn more about the different types of evidence in Audit Manager, see [Evidence](#) in the *Concepts and terminology* section of this guide.

How to add manual evidence

You can use any of the following methods to add your own manual evidence to an assessment control.

Keep in mind the following:

- You can only use one method at a time to add manual evidence.
- The maximum supported size for a single manual evidence file is 100 MB.
- The [Supported file formats for manual evidence \(p. 73\)](#) are listed further down this page.
- Each AWS account can only manually upload up to 100 evidence files to a control each day. Exceeding this daily quota causes any additional manual uploads to fail for that control. If you need to upload a large amount of manual evidence to a single control, upload your evidence in batches across several days.
- When a control is *inactive*, you can't add manual evidence to that control. To add manual evidence, you must first change the control status to either *under review* or *reviewed*. For instructions, see [Update control status \(p. 61\)](#).

Import a file from Amazon S3

Follow these steps to import manual evidence from an S3 bucket.

AWS console

To import a file from S3 (console)

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the left navigation pane, choose **Assessments**, and then choose the name of your assessment to open it.
3. Choose the **Controls** tab, scroll down to **Control sets**, and then choose the name of a control to open it.
4. On the **Evidence folders** tab, choose **Add manual evidence**, and then choose **Import file from S3**.
 - Alternatively, choose an evidence folder name in the **Evidence folders** tab to review the evidence folder summary, and then choose **Add manual evidence**, **Import file from S3**.
5. On the next page, enter the S3 URI of the evidence. You can find the S3 URI by navigating to the object in the [Amazon S3 console](#) and choosing **Copy S3 URI**.
6. Choose **Upload**.

AWS CLI

In the following procedure, replace the *placeholder text* with your own information.

To import a file from S3 (CLI)

1. Run the [`list-assessments`](#) command to see a list of your assessments.

```
aws auditmanager list-assessments
```

In the response, find the assessment that you want to upload evidence to and take note of the assessment ID.

2. Run the [`get-assessment`](#) command and specify the assessment ID from step one.

```
aws auditmanager get-assessment --assessment-id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

In the response, find the control set and the control that you want to upload evidence to, and take note of their IDs.

3. Run the [`batch-import-evidence-to-assessment-control`](#) command with the following parameters:

- `--assessment-id` – Use the assessment ID from step one.
- `--control-set-id` – Use the control set ID from step two.
- `--control-id` – Use the control ID from step two.
- `--manual-evidence` – Use `s3ResourcePath` as the manual evidence type and specify the S3 URI of the evidence. You can find the S3 URI by navigating to the object in the [Amazon S3 console](#) and choosing **Copy S3 URI**.

```
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://  
example-bucket/example-file.extension
```

Audit Manager API

To import a file from S3 (API)

1. Call the [ListAssessments](#) operation to see a list of your assessments. In the response, find the assessment that you want to upload evidence to and take note of the assessment ID.
2. Call the [GetAssessment](#) operation and specify the assessment ID from step one. In the response, find the control set and the control that you want to upload evidence to, and take note of their IDs.
3. Call the [BatchImportEvidenceToAssessmentControl](#) operation with the following parameters:
 - [assessmentId](#) – Use the assessment ID from step one.
 - [controlSetId](#) – Use the control set ID from step two.
 - [controlId](#) – Use the control ID from step two.
 - [manualEvidence](#) – Use s3ResourcePath as the manual evidence type and specify the S3 URI of the evidence. You can find the S3 URI by navigating to the object in the [Amazon S3 console](#) and choosing [Copy S3 URI](#).

For more information, choose any of the previous links to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Upload a file from your browser

Follow these steps to upload manual evidence from your browser.

AWS console

To upload a file from your browser (console)

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the left navigation pane, choose **Assessments**, and then choose the name of your assessment to open it.
3. On the **Controls** tab, scroll down to **Control sets**, and then choose the name of a control to open it.

From here, there are three ways to upload a file:

- (Option 1) In the blue notification banner, choose **Upload manual evidence**.
 - (Option 2) On the **Evidence folders** tab, choose **Add manual evidence**, and then choose **Upload file from browser**.
 - (Option 3) Choose an evidence folder name to review a summary of that folder, choose **Add manual evidence**, and then choose **Upload file from browser**.
4. Choose the file that you want to upload.
 5. Choose **Upload**.

AWS CLI

In the following procedure, replace the *placeholder text* with your own information.

To upload a file from your browser (CLI)

1. Run the [list-assessments](#) command to see a list of your assessments.

```
aws auditmanager list-assessments
```

In the response, find the assessment that you want to upload evidence to and take note of the assessment ID.

2. Run the [get-assessment](#) command and specify the assessment ID from step one.

```
aws auditmanager get-assessment --assessment-id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

In the response, find the control set and the control that you want to upload evidence to, and take note of their IDs.

3. Run the [get-evidence-file-upload-url](#) command and specify the file that you want to upload.

```
aws auditmanager get-evidence-file-upload-url --file-name fileName.extension
```

In the response, take note of the presigned URL and the evidenceFileName.

4. Use the presigned URL from step three to upload the file from your browser. This action uploads your file to Amazon S3, where it's saved as an object that can be attached to an assessment control. In the following step, you'll reference the newly-created object by using the evidenceFileName parameter.

Note

When you upload a file using a presigned URL, Audit Manager protects and stores your data by using server side encryption with AWS Key Management Service. To support this, you must use the x-amz-server-side-encryption header in your request when you use the presigned URL to upload your file.

If you're using a customer managed AWS KMS key in your Audit Manager [Data encryption \(p. 252\)](#) settings, make sure that you also include the x-amz-server-side-encryption-aws-kms-key-id header in your request. If the x-amz-server-side-encryption-aws-kms-key-id header isn't present in the request, Amazon S3 assumes that you want to use the AWS managed key.

For more information, see [Protecting data using server-side encryption with AWS Key Management Service keys \(SSE-KMS\)](#) in the *Amazon Simple Storage Service User Guide*.

5. Run the [batch-import-evidence-to-assessment-control](#) command with the following parameters:

- --assessment-id – Use the assessment ID from step one.
- --control-set-id – Use the control set ID from step two.
- --control-id – Use the control ID from step two.
- --manual-evidence – Use evidenceFileName as the manual evidence type and specify the evidence file name from step three.

```
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

To upload a file from your browser (API)

1. Call the [ListAssessments](#) operation. In the response, find the assessment that you want to upload evidence to and take note of the assessment ID.
2. Call the [GetAssessment](#) operation and specify the assessmentId from step one. In the response, find the control set and the control that you want to upload evidence to, and take note of their IDs.
3. Call the [GetEvidenceFileUploadUrl](#) operation and specify the fileName that you want to upload. In the response, take note of the presigned URL and the evidenceFileName.
4. Use the presigned URL from step three to upload the file from your browser. This action uploads your file to Amazon S3, where it's saved as an object that can be attached to an assessment control. In the following step, you'll reference the newly-created object by using the evidenceFileName parameter.

Note

When you upload a file using a presigned URL, Audit Manager protects and stores your data by using server side encryption with AWS Key Management Service. To support this, you must use the x-amz-server-side-encryption header in your request when you use the presigned URL to upload your file.

If you're using a customer managed AWS KMS key in your Audit Manager [Data encryption \(p. 252\)](#) settings, make sure that you also include the x-amz-server-side-encryption-aws-kms-key-id header in your request. If the x-amz-server-side-encryption-aws-kms-key-id header isn't present in the request, Amazon S3 assumes that you want to use the AWS managed key.

For more information, see [Protecting data using server-side encryption with AWS Key Management Service keys \(SSE-KMS\)](#) in the *Amazon Simple Storage Service User Guide*.

5. Call the [BatchImportEvidenceToAssessmentControl](#) operation with the following parameters:
 - [assessmentId](#) – Use the assessment ID from step one.
 - [controlSetId](#) – Use the control set ID from step two.
 - [controlId](#) – Use the control ID from step two.
 - [manualEvidence](#) – Use evidenceFileName as the manual evidence type and specify the evidence file name from step three.

For more information, choose any of the previous links to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Enter a text response

Follow these steps to enter a response to a risk assessment question and save your response as manual evidence.

AWS console

To enter a text response (console)

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the left navigation pane, choose **Assessments**, and then choose the name of your assessment to open it.
3. Choose the **Controls** tab, scroll down to **Control sets**, and then choose the name of a control to open it.

From here, there are three ways to enter a text response:

- (Option 1) In the blue notification banner, choose **Enter response**.
 - (Option 2) On the **Evidence folders** tab, choose **Add manual evidence**, and then choose **Enter text response**.
 - (Option 3) Choose an evidence folder to review a summary of that folder, choose **Add manual evidence**, and then choose **Enter text response**.
4. In the pop-up window that appears, enter your response in plain text format.
 5. Choose **Confirm**.

AWS CLI

In the following procedure, replace the *placeholder text* with your own information.

To enter a text response (CLI)

1. Run the [list-assessments](#) command.

```
aws auditmanager list-assessments
```

In the response, find the assessment that you want to upload evidence to and take note of the assessment ID.

2. Run the [get-assessment](#) command and specify the assessment ID from step one.

```
aws auditmanager get-assessment --assessment-id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

In the response, find the control set and control that you want to upload evidence to, and take note of their IDs.

3. Run the [batch-import-evidence-to-assessment-control](#) command with the following parameters:

- **--assessment-id** – Use the assessment ID from step one.
- **--control-set-id** – Use the control set ID from step two.
- **--control-id** – Use the control ID from step two.
- **--manual-evidence** – Use `textResponse` as the manual evidence type and enter the text that you want to save as manual evidence.

```
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

To enter a text response (API)

1. Call the [ListAssessments](#) operation. In the response, find the assessment that you want to upload evidence to and take note of the assessment ID.
2. Call the [GetAssessment](#) operation and specify the assessmentId from step one. In the response, find the control set and control that you want to upload evidence to, and take note of their IDs.
3. Call the [BatchImportEvidenceToAssessmentControl](#) operation with the following parameters:
 - [assessmentId](#) – Use the assessment ID from step one.
 - [controlSetId](#) – Use the control set ID from step two.
 - [controlId](#) – Use the control ID from step two.
 - [manualEvidence](#) – Use textResponse as the manual evidence type and enter the text that you want to save as manual evidence.

For more information, choose any of the previous links to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Supported file formats for manual evidence

The following table lists and describes the types of file that you can upload as manual evidence. For each file type, the table also lists the supported file extensions.

File type	Description	Supported file extensions
Compression or archive	GNU Zip compressed archives and ZIP compressed archives	.gz, .zip
Document	Common document files such as PDFs and Microsoft Office files	.doc, .docx, .pdf, .ppt, .pptx, .xls, .xlsx
Image	Image and graphic files	.jpeg, .jpg, .png, .svg
Text	Other non-binary text files, such as plain-text documents and markup language files	.cer, .csv, .html, .jmx, .json, .md, .out, .rtf, .txt, .xml, .yaml, .yml

Generating an assessment report

An assessment report summarizes your assessment and provides links to an organized set of folders that contain related evidence. For more information, see [Assessment reports \(p. 85\)](#).

You can choose which evidence you want to include in your assessment report before you generate the assessment report. Newly collected evidence isn't automatically included in an assessment report.

Tasks

- [Adding evidence to an assessment report \(p. 74\)](#)
- [Removing evidence from an assessment report \(p. 74\)](#)
- [Generating an assessment report \(p. 75\)](#)
- [What can I do next? \(p. 75\)](#)

Adding evidence to an assessment report

Before you can generate an assessment report, you must add at least one piece of evidence to your assessment report. You can either add an entire evidence folder, or you can add individual evidence items from within a folder.

To add evidence to an assessment report

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Assessments** and then choose the name of the assessment to open it.
3. On the **Controls** tab, scroll down to the **Control sets** table and choose the name of a control to open it.
4. Choose how you want to add evidence to your assessment report.
 - a. To add an entire evidence folder, scroll down to **Evidence folders**, select the folder that you want to add, and then choose **Add to assessment report**.
 - If you can't see the folder that you're looking for, change the dropdown filter to **All time**. Otherwise, you'll see the last seven days of folders by default.
 - If **Add to assessment report** is greyed out, the evidence folder was already added to the assessment report.
 - b. To add specific evidence, choose an evidence folder to open its contents. Select one or more items from the list, and then choose **Add to assessment report**.
 - If **Add to assessment report** is greyed out, make sure that you selected the check box next to the evidence, and then try again.
5. After you add the evidence to the assessment report, a green success banner appears. Choose **View evidence in assessment report** to see the evidence that will be included in your assessment report.
 - Alternatively, you can see the evidence that will be included in your assessment report by navigating back to your assessment and choosing the **Assessment report selection** tab.

Removing evidence from an assessment report

If you need to remove evidence from an assessment report, follow these steps. You can either remove an entire evidence folder, or you can remove specific evidence items from within a folder.

To remove evidence from an assessment report

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Assessments** and then choose the name of the assessment to open it.
3. On the **Controls** tab, scroll down to the **Control sets** table and choose the name of a control to open it.
4. Choose how you want to remove evidence from your assessment report.

- a. To remove an entire evidence folder, scroll down to **Evidence folders**, select the folder that you want to remove, and then choose **Remove from assessment report**.
 - If you can't see the folder that you're looking for, change the dropdown filter to **All time**. Otherwise, you'll see the last seven days of folders by default.
 - If **Remove from assessment report** is greyed out, the evidence folder was already removed from the assessment report.
 - b. To remove specific evidence, choose an evidence folder to open its contents. Select one or more items from the list, and then choose **Remove from assessment report**.
 - If **Remove from assessment report** is greyed out, make sure that you selected the check box next to the evidence, and then try again.
5. After you add the evidence to the assessment report, a green success banner appears. Choose **View evidence in assessment report** to see the evidence that will be included in your assessment report.
 - Alternatively, you can see the evidence that will be included in your assessment report by navigating back to your assessment and choosing the **Assessment report selection tab**.

Generating an assessment report

After you add evidence to your assessment report, you can generate the final assessment report to share with your auditors. When you generate an assessment report, it's placed into the S3 bucket that you chose as your assessment report destination.

Tip

To ensure that your assessment report is generated successfully, review our [Configuration tips for your assessment report destination \(p. 261\)](#).

To generate an assessment report

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the left navigation pane, choose **Assessments**.
3. Choose the name of the assessment that you want to generate an assessment report for.
4. Choose the **Assessment report selection tab**, and then choose **Generate assessment report**.
 - If **Generate assessment report** is greyed out, this means that no evidence was added to the assessment report yet.
5. In the pop-up window, provide a name and description for the assessment report, and review the assessment report details.
6. Choose **Generate assessment report** and wait a few minutes while your assessment report is generated.
7. Find and download your assessment report from the **Download center** page of the Audit Manager console.
 - Alternatively, you can go to your assessment report destination S3 bucket and download the assessment report from there.

The assessment report has a file checksum to ensure the integrity of the assessment report. You can validate this with the [ValidateAssessmentReportIntegrity](#) API operation that's provided by Audit Manager.

What can I do next?

After you generate an assessment report, you can learn more about the following:

- **Find and download your assessment report** – Learn how to download your assessment report [from the download center](#) or [from Amazon S3](#).
- **Explore your assessment report** – Learn how to [navigate an assessment report and explore its contents](#).
- **Validate your assessment report** – Learn how to use the [ValidateAssessmentReportIntegrity](#) API operation to validate your assessment report.
- **Delete an unwanted assessment report** – Learn how to delete an unwanted report [from the download center](#) or [from Amazon S3](#).

Changing the status of an assessment to inactive

When you no longer need Audit Manager to collect evidence, you can stop ongoing evidence collection for your assessment. You can do this by changing the assessment status to *Inactive*.

In addition to stopping evidence collection, Audit Manager makes the following changes to the controls that are within the inactive assessment:

- All control sets change to *Reviewed* status.
- All controls that are *Under review* change to *Reviewed* status.
- Delegates for the inactive assessment can no longer view or edit its controls and control sets.

Warning

We recommend that you proceed with caution and make sure that you want to mark your assessment as inactive. When an assessment is inactive, you have read-only access to its contents. You can still view previously collected evidence and generate assessment reports. However, you can't make any changes, add comments, or upload manual evidence.

Audit Manager console

To change an assessment status to inactive (console)

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Assessments**.
3. Choose the name of the assessment to open it.
4. On the upper-right corner of the page, choose **Update assessment status**, and then choose **Inactive**.
5. Choose **Update status** in the pop-up window to confirm that you want to change the status to inactive.

The changes to the assessment and its controls take effect after approximately one minute.

AWS CLI

To change an assessment status to inactive (AWS CLI)

1. First, identify the assessment that you want to update. To do this, run the [list-assessments](#) command.

```
aws auditmanager list-assessments
```

The response returns a list of assessments. Find the assessment that you want to deactivate, and take note of the assessment ID.

2. Next, run the [update-assessment-status](#) command and specify the following parameters:

- `--assessment-id` – Use this parameter to specify the assessment that you want to deactivate.
- `--status` – Set this value to INACTIVE.

In the following example, replace the *placeholder text* with your own information.

```
aws auditmanager update-assessment-status --assessment-id a1b2c3d4-5678-90ab-cdef-  
EXAMPLE1111 --status INACTIVE
```

The changes to the assessment and its controls take effect after approximately one minute.
Audit Manager API

To change an assessment status to inactive (API)

1. Use the [ListAssessments](#) operation to find the assessment that you want to deactivate, and take note of the assessment ID.
2. Use the [UpdateAssessmentStatus](#) operation and specify the following parameters:
 - `assessmentId` – Use this parameter to specify the assessment that you want to deactivate.
 - `status` – Set this value to INACTIVE.

The changes to the assessment and its controls take effect after approximately one minute.

For more information about these API operations, choose any of the previous links to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Deleting an assessment

You can delete an assessment that you no longer want in Audit Manager. You can delete assessments using the Audit Manager console, the Audit Manager API or the AWS Command Line Interface (AWS CLI).

Audit Manager console

To delete an assessment (console)

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Assessments**.
3. Select the assessment that you want to delete, and choose **Delete**.
 - Alternatively, you can open the assessment and then choose **Delete** in the top right of the page.

AWS CLI

To delete an assessment (AWS CLI)

1. First, identify the assessment that you want to delete. To do this, run the [list-assessments](#) command.

```
aws auditmanager list-assessments
```

The response returns a list of assessments. Find the assessment that you want to delete, and take note of the assessment ID.

2. Next, use the [delete-assessment](#) command and specify the --assessment-id of the assessment that you want to delete.

In the following example, replace the *placeholder text* with your own information.

```
aws auditmanager delete-assessment --assessment-id a1b2c3d4-5678-90ab-cdef-  
EXAMPLE11111
```

Audit Manager API

To delete an assessment (API)

1. Use the [ListAssessments](#) operation to find the assessment that you want to delete.
In the response, take note of the assessment ID.
2. Use the [DeleteAssessment](#) operation and specify the [assessmentId](#) of the assessment that you want to delete.

For more information about these API operations, choose any of the previous links to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Delegations in AWS Audit Manager

Audit owners use AWS Audit Manager to create assessments and collect evidence for the controls that are listed in that assessment. Sometimes audit owners might have questions or need assistance when validating the evidence for a control set. In this situation, an audit owner can delegate a control set to a subject matter expert for review.

At a high level, the delegation process is as follows.

1. The audit owner chooses a control set in their assessment and delegates it for review.
2. The delegate reviews those controls and their evidence, and submits the control set back to the audit owner when finished.
3. The audit owner is notified that the review is complete, and checks the reviewed controls for any remarks from the delegate.

Use the following sections of this guide to learn more about how to manage delegation tasks in AWS Audit Manager.

Topics

- [Delegation tasks for audit owners \(p. 79\)](#)
- [Delegation tasks for delegates \(p. 82\)](#)

Note

An account can be an audit owner or a delegate in different AWS Regions.

Delegation tasks for audit owners

As an audit owner in AWS Audit Manager, you might need assistance from a subject matter expert to help you review controls and evidence. In this situation, you can delegate a control set for review.

The following topics describe how you can manage delegations in AWS Audit Manager.

Delegation tasks

- [Delegating a control set for review \(p. 79\)](#)
- [Accessing your active and completed delegations \(p. 80\)](#)
- [Deleting your active and completed delegations \(p. 81\)](#)

Delegating a control set for review

When you need assistance from a subject matter expert, you can choose the AWS account that you want to help you, and then delegate a control set to them for review.

You can use either of the following procedures to delegate a control set.

Delegating a control set from an assessment page

To delegate a control set from the assessment page

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Assessments**.
3. Select the name of the assessment that contains the control set that you want to delegate.
4. From the assessment page, choose the **Controls** tab. This displays the control status summary and the list of controls in the assessment.
5. Select a control set and choose **Delegate control set**.
6. Under **Delegate selection**, a list of users and roles is displayed. Choose a user or role, or use the search bar to look for one.
7. Under **Delegation details**, review the control set name and the assessment name.
8. (Optional) Under **Comments**, add a comment with instructions to help the delegate fulfill their review task. Don't include any sensitive information in your comment.
9. Choose **Delegate control set**.
10. A green success banner confirms the successful delegation of the control set. Choose **View delegation** to see the delegation request. You can also view your delegations at any time by choosing **Delegations** in the left navigation pane of the AWS Audit Manager console.

Delegating a control set from the delegations page

To delegate a control set from the delegations page

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Delegations**.
3. From the delegations page, choose **Create delegation**.
4. Under **Choose assessment and control set**, specify the assessment and the control set that you want to delegate.
5. Under **Delegate selection**, you will see a list of users and roles. Choose a user or role, or use the search bar to look for one.
6. (Optional) Under **Comments**, add a comment with instructions to help the delegate fulfill their review task. Don't include any sensitive information in your comment.
7. Choose **Create delegation**.
8. A green success banner confirms the successful delegation of the control set. Choose **View delegation** to see the delegation request. You can also view your delegations at any time by choosing **Delegations** in the left navigation pane of the AWS Audit Manager console.

When you delegate a control set for review, the delegate receives a notification and can then begin to review the control set. This process that delegates follow is described in [Delegation tasks for delegates \(p. 82\)](#).

Tip

Delegates can subscribe to an SNS topic to receive email alerts when a review task is delegated to them. For more information about how to identify and subscribe to the SNS topic that's associated with AWS Audit Manager, see [Notifications in AWS Audit Manager](#).

Accessing your active and completed delegations

You can access a list of your delegations at any time by choosing **Delegations** in the left navigation pane of AWS Audit Manager. The delegations page contains a list of your active and completed delegations, with the following details for each delegation:

- **Delegated to** – The AWS account that you delegated the control set to.
- **Date** – The date when you delegated the control set.
- **Status** – The current status of the delegation.
- **Assessment** – The name of the assessment with a link to the assessment detail page.
- **Control set** – The name of the control set that was delegated for review.

When a delegation is completed, you receive a notification in AWS Audit Manager. You may also receive comments with remarks from the delegate. The following procedure explains how to check your notifications in Audit Manager after a delegation is completed, and how to view any comments that the delegate might have left for you.

To view a completed delegation and check for comments

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Notifications**. Or, choose **Notifications** in the blue flash bar at the top of the screen to open the notifications page.
3. Review the **Notifications** page, which includes a table with the following information:
 - **Date** – The date of the notification.
 - **Assessment** – The name of the assessment that's associated with the control set.
 - **Control set** – The name of the control set.
 - **Source** – The user or role of the delegate who submitted the completed control set back to you.
 - **Description** – High-level remarks provided by the delegate.
4. Find the assessment and control set that the delegate reviewed and submitted to you, and choose the name of the assessment to open it.
5. Under the **Controls** tab of the assessment detail page, scroll down to the **Control sets** table. Under the **Controls grouped by control set** column, expand the name of a control set to show its controls. Then, choose the name of a control to open the control detail page.
6. Choose the **Comments** tab to view any remarks added by the delegate for that particular control.
7. When you are satisfied that the review is complete for a control set, select the control set and choose **Complete control set review**.

Important

Audit Manager collects evidence continuously. As a result, additional new evidence might be collected *after* the delegate completes their review of a control.

If you only want to use reviewed evidence in your assessment reports, you can refer to the *control reviewed* timestamp to determine when evidence was reviewed. This timestamp can be found on the [Changelog tab](#) of the control detail page. You can then use this timestamp to identify which evidence you add to your assessment reports.

Deleting your active and completed delegations

There may be circumstances where you create a delegation but later no longer need assistance reviewing that control set. When this happens, you can delete an active delegation in AWS Audit Manager. You can also delete completed delegations that you no longer want to appear on the delegations page.

To delete a delegation

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Delegations**.
3. On the **Delegations** page, select the delegation that you want to cancel and then choose **Remove delegation**.

4. In the pop-up window that appears, choose **Delete** to confirm your choice.

Delegation tasks for delegates

Delegates typically have specialized business or technical expertise in several different areas. These include data retention policies, training plans, network infrastructure, and identity management. They can help audit owners review collected evidence for controls that fall under their area of expertise.

As a delegate, you might receive requests from audit owners to review the evidence that's associated with a control set. This request indicates that the audit owner needs your assistance with validating this evidence. You can help audit owners by reviewing control sets and their related evidence, adding comments, uploading additional evidence, and updating the status of each control that you review.

The following topics describe how you can manage delegations in AWS Audit Manager.

Note

Audit owners delegate specific control sets for review, not entire assessments. As a result, delegates have limited access to assessments. Delegates can review evidence, add comments, upload manual evidence, and update the control status for each of the controls in the control set. For more information about roles and permissions in Audit Manager, see [Recommended policies for user personas in AWS Audit Manager \(p. 317\)](#).

Delegation tasks

- [Viewing your notifications for incoming delegation requests \(p. 82\)](#)
- [Reviewing the delegated control set and its related evidence \(p. 83\)](#)
- [Adding a comment to a control \(p. 83\)](#)
- [Marking a control as reviewed \(p. 84\)](#)
- [Submitting the reviewed control set back to the audit owner \(p. 84\)](#)

Viewing your notifications for incoming delegation requests

When an audit owner requests your assistance with reviewing a control set, you receive a notification that informs you of the control set that they delegated to you.

Tip

You can also subscribe to an SNS topic to receive email alerts when a control set is delegated to you for review. For more information, see [Notifications in AWS Audit Manager](#).

To view your notifications

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. Choose **Notifications** in the left navigation pane. Or, in the blue flash bar at the top of the screen, choose **View notification** to open the notifications page.
3. On the **Notifications** page, review the list of control sets that have been delegated to you for review. The table includes the following information:
 - **Date** – The date when the control set was delegated.
 - **Assessment** – The name of the assessment that's associated with the control set.
 - **Control set** – The name of the control set.
 - **Source** – The user or role that delegated the control set to you.
 - **Description** – Instructions that are provided by the audit owner.

Reviewing the delegated control set and its related evidence

You can assist audit owners by reviewing the control sets that they have delegated to you. You can examine these controls and their related evidence to determine if any additional action is needed. Such additional action could include [manually uploading additional evidence](#) to demonstrate compliance, or [leaving a comment](#) that details the remediation steps that you followed.

To review a control set

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Notifications**. Or, in the blue flash bar, choose **View notification** to open the notifications page.
3. On the **Notifications** page, a list of control sets that were delegated to you is displayed. Identify which control set you want to review, and choose the name of the related assessment to open the assessment detail page.
4. Under the **Controls** tab of the assessment detail page, scroll down to the **Control sets** table.
5. Under the **Controls grouped by control set** column, expand the name of a control set to show its controls, and choose the name of a control to open the control detail page.
6. (Optional) Choose **Update control status** to change the status of the control. While your review is in progress, you can mark the status as **Under Review**.
7. Review information about the control in the **Evidence folders**, **Data sources**, **Comments**, and **Changelog** tabs. For information about each of these tabs and how to interpret this information, see [Reviewing the controls in an assessment](#).

To review the evidence for a control

1. From the control detail page, choose the **Evidence folders** tab.
2. Navigate to the **Evidence folders** table, a list of folders that contain evidence for that control are displayed. These folders are organized and named based on the date when the evidence was collected.
3. Choose the name of an evidence folder to open it. Then, review a summary of all evidence gathered on that date. This summary includes the total number of compliance check issues that were reported directly from AWS Security Hub, AWS Config, or both. For instructions on how to interpret the data on this page, see [Reviewing evidence folders](#).
4. From the evidence folder summary page, navigate to the **Evidence** table. Under the **Time** column, choose a line item to open. Then, review the details about the piece of evidence that was collected at that time. For instructions on how to interpret the data on an evidence detail page, see [Reviewing individual evidence](#).

Tip

Although AWS Audit Manager automatically collects evidence for many controls, in some cases you might need to provide additional evidence to demonstrate compliance. In these cases, you can manually upload evidence. For instructions, see [Uploading manual evidence](#).

Adding a comment to a control

You can add comments for any controls that you review. These comments are visible to the audit owner.

To add a comment to a control

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.

2. Choose **Notifications** in the left navigation pane. Or, choose **View notification** in the blue flash bar at the top of the screen to open the notifications page.
3. On the **Notifications** page, review the list of control sets that were delegated to you. Find the control set that contains the control that you want to leave a comment for, and choose the name of the related assessment.
4. Choose the **Controls** tab, scroll down to the **Control sets** table, and then select the name of a control to open it.
5. Choose the **Comments** tab.
6. Under **Send comments**, enter your comment in the text box.
7. Choose **Submit comment** to add your comment. Then, your comment appears under the **Previous comments** section of the page, along with any other comments regarding this control.

Marking a control as reviewed

You can indicate your review progress by updating the status of individual controls within a control set. Changing the control status is optional. However, we recommend that you change the status of each control to **Reviewed** as you complete your review for that control. Regardless of the status of each individual control, you can still submit the controls back to the audit owner.

To mark a control as reviewed

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. Choose **Notifications** in the left navigation pane. Or, choose **View notification** in the blue flash bar at the top of the screen to open the notifications page.
3. On the **Notifications** page, review the list of control sets that were delegated to you. Find the control set that you want to mark as reviewed, and choose the name of the related assessment.
4. Under the **Controls** tab of the assessment detail page, scroll down to the **Control sets** table.
5. Under the **Controls grouped by control set** column, expand the name of a control set to show its controls. Choose the name of a control to open the control detail page.
6. Choose **Update control status** and change the status to **Reviewed**.
7. In the pop-up window that appears, choose **Update control status** to confirm that you finished reviewing the control.

Submitting the reviewed control set back to the audit owner

When you are done reviewing the controls that were delegated to you, submit the control set to the audit owner. This completes the delegation process.

To submit a reviewed control set back to the audit owner

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. Choose **Notifications** in the left navigation pane.
3. Review the list of control sets that were delegated to you. Find the control set that you want to submit back to the audit owner, and choose the name of the related assessment.
4. Scroll down to the **Control sets** table, select the control set that you want to submit to the audit owner, and then choose **Submit for review**.
5. In the pop-up window that appears, you can add comments before choosing **Submit for review**. After you submit the control to the audit owner, they can view any comments that you left for them.

Assessment reports

An *assessment report* summarizes the selected evidence that was collected for an assessment. It also contains links to PDF files with details about each piece of evidence. The specific contents, organization, and naming convention of an assessment report depend on the parameters that you choose when you [generate the report](#).

Assessment reports help you to select and compile the evidence that's relevant for your audit. However, they don't assess the compliance of the evidence itself. Instead, Audit Manager simply provides the selected evidence details as an output that you can share with your auditor.

Assessment report folder structure

When you download an assessment report, Audit Manager produces a zip folder. This contains your assessment report and related evidence files in nested subfolders.

The zip folder is structured as follows:

- **Assessment folder** (example: myAssessmentName-a1b2c3d4) – The root folder.
- **Assessment report folder** (example: reportName-a1b2c3d4e5f6g7) – A subfolder where you can find the AssessmentReportSummary.pdf, digest.txt, and README.txt files.
- **Evidence by control folder** (example: controlName-a1b2c3d4e5f6g) – A subfolder that groups evidence files by the related control.
 - **Evidence by data source folder** (example: CloudTrail, Security Hub) – A subfolder that groups evidence files by the data source type.
 - **Evidence by date folder** (example: 2022-07-01) – A subfolder that groups evidence files by the evidence collection date.
 - **Evidence files** – The files that contain details about individual pieces of evidence.

How to navigate an assessment report

Start by opening the zip folder and navigating one level down to the assessment report folder. Here, you can find the assessment report PDF and the README.txt file.

You can review the README.txt file to understand the structure and the contents of the zip folder. It also provides reference information about the naming conventions for each file. This information can help you navigate directly to a subfolder or evidence file if you're looking for a specific item.

Otherwise, to browse evidence and locate the information that you need, open the assessment report PDF. This gives you a high-level overview of the report, and a summary of the assessment that the report was created from.

Next, use the table of contents (TOC) to explore the report. You can choose any hyperlinked control in the TOC to jump directly to a summary of that control.

When you're ready to review evidence details for a control, you can do so by choosing the hyperlinked evidence name. For automated evidence, the hyperlink opens a new PDF file with details about that evidence. For manual evidence, the hyperlink takes you to the S3 bucket that contains the evidence.

Tip

The breadcrumb navigation at the top of each page shows your current location in the assessment report as you browse controls and evidence. Select the hyperlinked TOC to navigate back to the TOC at any time.

Assessment report sections

Use the following information to learn more about each section of an assessment report.

Note

When you see a hyphen (-) next to any of the attributes in the following sections, this indicates that the value of that attribute is null, or a value doesn't exist.

- [Cover page \(p. 86\)](#)
- [Overview page \(p. 86\)](#)
- [Table of contents page \(p. 87\)](#)
- [Control page \(p. 87\)](#)
- [Evidence summary page \(p. 88\)](#)
- [Evidence detail page \(p. 89\)](#)

Cover page

The cover page includes the name of the assessment report. It also displays the date and time that the report was generated, along with the account ID of the user who generated the report.

The cover page is formatted as follows. Audit Manager replaces the *placeholders* with the information that's relevant to your report.

Assessment report name
Report generated on *MM/DD/YYYY* at *HH:MM:SS AM/PM UCT* by *AccountID*

Overview page

The overview page has two parts: a summary of the report itself, and a summary of the assessment that's being reported on.

Report summary

This section summarizes the assessment report.

- **Report name** – The name of the report.
- **Description** – The description that's entered by the audit owner when they generate the report.
- **Date generated** – The date when the report was generated. The time is represented in Coordinated Universal Time (UTC).
- **Total controls included** – The number of controls that are included in the report and have collected evidence. This is a subset of the total number of controls in the assessment.
- **AWS accounts included** – The number of AWS accounts that are included in the report and have collected evidence. This is a subset of the total number of AWS accounts in the assessment.
- **Assessment report selection** – The number of evidence items that are selected for inclusion in the report. This includes the total number of compliance check issues that are found in the report.

Assessment summary

This section summarizes the assessment that the report relates to.

- **Assessment name** – The name of the assessment that the report was generated from.
- **Status** – The status of the assessment at the time when the report was generated.
- **Assessment Region** – The AWS Region that the assessment was created in.
- **AWS accounts in scope** – The full list of AWS accounts that are in the scope of the assessment.
- **AWS services in scope** – The full list of AWS services that are in the scope of the assessment.
- **Framework name** – The name of the framework that the assessment was created from.
- **Audit owners** – The user or role of the assessment's audit owners.
- **Last updated** – The date when the assessment was last updated. The time is represented in UTC.

Table of contents page

The TOC displays the full contents of the assessment report. The contents are grouped and organized based on the control sets that are included in the assessment. Controls are listed underneath their respective control set.

Choose any item in the table of contents to navigate directly to that section of the report. You can either choose a control set or go directly to a control.

Control page

The control page has two parts: a summary of the control itself, and a summary of the evidence that was collected for the control.

Control summary

This section includes the following information.

- **Control name** – The name of the control.
- **Description** – The description of the control.
- **Control set** – The name of the control set that the control belongs to.
- **Testing information** – The recommended testing procedures for this control.
- **Action plan** – The recommended actions to perform if the control isn't fulfilled.
- **Assessment report selection** – The number of evidence items related to this control that were included in the assessment report. This includes the number of compliance check issues that were found for this control's evidence.

Collected evidence

This section shows the evidence that was collected for the control. The evidence is grouped by folders, which are organized and named by the evidence collection date. Next to each evidence folder name is the total number of compliance check issues for that folder.

Underneath each evidence folder name is a list of hyperlinked evidence names.

- Automated evidence names start with an evidence collection timestamp, followed by the service code, event name (up to 20 characters), account ID, and a unique 12-character unique ID.

For example: 21-30-24_IAM_CreateUser_111122223333_a1b2c3d4e5f6

For automated evidence, the hyperlinked name opens a new PDF file with a summary and further details.

- Manual evidence names start with an evidence upload timestamp, followed by the manual label, account ID, and a 12-character unique ID. They also include the first 10 characters of the file name, and the file extension (up to 10 characters).

For example: 00-00-00_manual_111122223333_a1b2c3d4e5f6_myimage.png

For manual evidence, the hyperlinked name takes you to the S3 bucket that contains that evidence.

Next to each evidence name is the result of the compliance check for that item.

- For automated evidence that's collected from AWS Security Hub or AWS Config, a **Compliant**, **Non-compliant**, or **Inconclusive** result is reported.
- For automated evidence that's collected from AWS CloudTrail and API calls, and for all manual evidence, an **Inconclusive** result is shown.

Evidence summary page

The evidence summary page includes the following information:

- **ID** – The unique identifier for the evidence.
- **Date collected** – The date when the evidence was created or uploaded.
- **Description** – A description of the evidence, including the account ID and the data source type.
- **Assessment name** – The name of the assessment that the report was generated from.
- **Framework name** – The name of the framework that the assessment was created from.
- **Control name** – The name of the control that the evidence supports.
- **Control set name** – The name of the control set that the related control belongs to.
- **Control description** – The description of the control that the evidence supports.
- **Testing information** – The recommended testing procedures for the control.
- **Action plan** – The recommended actions to perform if the control is not fulfilled.
- **AWS Region** – The name of the Region that's associated with the evidence.
- **IAM ID** – The ARN of the user or role that's associated with the evidence.
- **AWS account** – The AWS account ID that's associated with the evidence.
- **AWS service** – The name of the AWS service that's associated with the evidence.
- **Resources included** – The AWS resources that were assessed to generate the evidence. This attribute isn't applicable for compliance check evidence from AWS Config. For this evidence type, you can find all of the resources tabulated in the [Evidence detail page \(p. 89\)](#) of the evidence PDF.
- **Event name** – The name of the evidence event.
- **Event time** – The time when the evidence event occurred.
- **Data source** – Where the evidence was collected or uploaded from. The data source type can be either AWS Config, Security Hub, AWS API calls, CloudTrail, or Manual.
- **Evidence by type** – The category of the evidence
 - *Compliance check* evidence is collected from AWS Config or Security Hub.
 - *User activity* evidence is collected from CloudTrail logs.
 - *Configuration data* evidence is collected from snapshots of other AWS services.
 - *Manual* evidence is evidence that you upload manually.

- **Compliance check status** – The evaluation status for evidence that falls under the *compliance check* category.
 - For automated evidence that's collected from AWS Security Hub or AWS Config, a **Compliant**, **Non-compliant**, or **Inconclusive** result is reported.
 - For automated evidence that's collected from AWS CloudTrail and API calls, and for all manual evidence, an **Inconclusive** result is shown.

Evidence detail page

The evidence detail page shows the name of the evidence and an evidence detail table. This table provides a detailed breakdown of each element of the evidence so that you can understand the data and validate that it's correct. Depending on the data source of the evidence, the contents of the evidence detail page vary.

Tip

The breadcrumb navigation at the top of each page shows your current location as you browse evidence details. Select **Evidence summary** to navigate back to the evidence summary at any time.

Assessment report integrity check

When you generate an assessment report, Audit Manager produces a report file checksum called `digest.txt`. You can use this file to validate the integrity of the report and ensure that no evidence was modified after the report was created. It contains a JSON object with signatures and hashes that are invalidated if any part of the report archive is altered.

To validate the integrity of an assessment report, use the [ValidateAssessmentReportIntegrity](#) API that's provided by Audit Manager.

Troubleshooting assessment reports

To find answers to common questions and issues, see [Troubleshooting assessment report issues](#) in the *Troubleshooting* section of this guide.

Evidence finder

Evidence finder provides a powerful way to search for evidence in Audit Manager. Instead of browsing deeply nested evidence folders to find what you're looking for, you can now use evidence finder to quickly query your evidence. If you use evidence finder as a delegated administrator, you can search for evidence across all member accounts in your organization.

Using a combination of filters and groupings, you can progressively narrow the scope of your search query. For example, if you want a high-level view of your system health, perform a broad search and filter by assessment, date range, and resource compliance. If your goal is to remediate a specific resource, you can perform a narrow search to target evidence for a specific control or resource ID. After you define your filters, you can group and then preview the matching search results before creating an assessment report.

To use evidence finder, you must enable this feature from your Audit Manager settings.

Topics

- [Understanding how evidence finder works with CloudTrail Lake \(p. 90\)](#)
- [Enabling evidence finder \(p. 91\)](#)
- [Troubleshooting evidence finder \(p. 91\)](#)
- [Searching for evidence \(p. 91\)](#)
- [Viewing results in evidence finder \(p. 93\)](#)
- [Filter and grouping options \(p. 99\)](#)
- [Example use cases \(p. 102\)](#)

Understanding how evidence finder works with CloudTrail Lake

Evidence finder uses [AWS CloudTrail Lake](#) querying and storage capability. Before you start using evidence finder, it's helpful to understand a little more about how CloudTrail Lake works.

CloudTrail Lake aggregates data into a single, searchable event data store that supports powerful SQL queries. This means that you can search for data across your organization and within custom time ranges. With evidence finder, you can use this search functionality directly in the Audit Manager console.

When you request to enable evidence finder, Audit Manager creates an event data store on your behalf. After evidence finder is enabled, all of your future Audit Manager evidence is ingested into the event data store where it's available for evidence finder search queries. After you enable evidence finder, we also backfill the newly created event data store with your past two years' worth of evidence data. If you enable evidence finder as a delegated administrator, we backfill the data for all member accounts in your organization.

All of your evidence data, whether backfilled or new, is retained in the event data store for 2 years. You can change the default retention period at any time. For instructions, see [Update an event data store](#) in the [AWS CloudTrail User Guide](#). You can keep data in an event data store for up to 7 years, or 2,555 days.

Note

The data backfill process, when this feature is enabled, is free of charge if completed by November 2023.

When new evidence data is added to the event data store moving forward, CloudTrail Lake charges are incurred for data storage and ingestion.

For CloudTrail Lake queries, you pay as you go. This means that for each search query that you run in evidence finder, you're charged for the data that's scanned.

For more information about CloudTrail Lake pricing, see [AWS CloudTrail pricing](#).

Enabling evidence finder

You can enable evidence finder from your Audit Manager settings. For instructions, see [Evidence finder](#) on the *AWS Audit Manager Settings* page of this guide.

Troubleshooting evidence finder

To find answers to common questions and issues, see [Troubleshooting evidence finder issues](#) in the *Troubleshooting* chapter of this guide.

Searching for evidence

Follow these steps to search for evidence in the Audit Manager console.

Note

You can also use the CloudTrail API to query your evidence data. For more information, see [StartQuery](#) in the *AWS CloudTrail API Reference*. If you prefer to use the AWS CLI, see [Start a query](#) in the *AWS CloudTrail User Guide*.

On this page

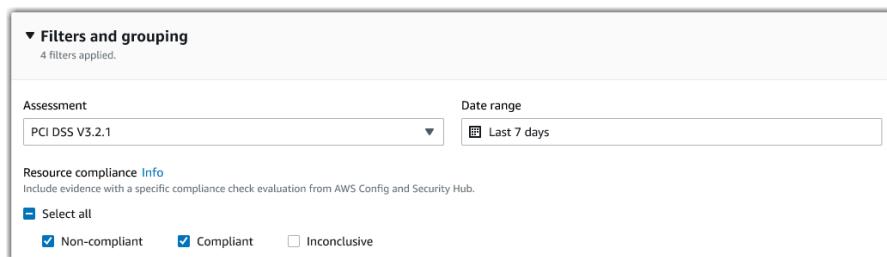
- [Performing a search query \(p. 91\)](#)
- [Stopping a search query \(p. 92\)](#)
- [Editing search filters \(p. 93\)](#)

Performing a search query

Follow these steps to perform a search query in evidence finder.

To search for evidence

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Evidence finder**.
3. Next, apply filters to narrow the scope of your search.
 - a. For **Assessment**, choose an assessment.
 - b. For **Date range**, select a range.
 - c. For **Resource compliance**, select an evaluation status.



4. (Optional) Choose **Additional filters - optional** to narrow the search even further.
 - a. Choose **Add criteria**, select a criteria, and then select one or more values for that criteria.
 - b. Continue to build more filters in the same way.
 - c. To remove an unwanted filter, choose **Remove**.

The screenshot shows a user interface for adding optional filters. At the top, there is a dropdown menu labeled 'Additional filters - optional'. Below it, a section titled 'Criteria' contains a 'Control' dropdown set to 'equals', a 'Value' dropdown set to 'Choose a control', and a 'Remove' button. A single criterion is listed: 'C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.' with a delete icon. At the bottom left is a 'Add criteria' button, and at the bottom center is a note: 'You can add 9 more criteria.'

5. Under **Grouping**, specify whether you want to group the search results.
 - a. If you want to group the results, select a value to group the results by.
 - b. If you don't want to group the results, proceed to step 6.



6. Choose **Search**.



Your search might take a few minutes, depending on the amount of evidence data that you have. Feel free to navigate away from evidence finder while the search is in progress. A flash bar notifies you when the search results are ready.

Tip

For more information about the filters and groupings that you can use in this procedure, see [Filter and grouping options](#).

Stopping a search query

If you want to stop a search query for any reason, follow these steps.

Note

Stopping a search query can still result in charges. You're charged for the amount of evidence data that was scanned before you stopped the search query. After it's stopped, you can view the partial results that were returned.

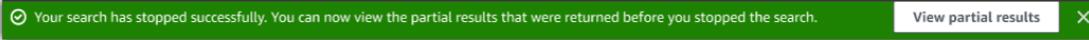
To stop an in-progress search query

1. In the blue progress flash bar at the top of the screen, choose **Stop search**.



2. (Optional) Review the partial results that were returned before you stopped the search query.

- a. If you're on the evidence finder page, the partial results are displayed on the screen.
- b. If you navigated away from evidence finder, choose **View partial results** in the green confirmation flash bar.



Editing search filters

You can return to your most recent search query and change the filters as needed.

Note

When you edit your filters and choose **Search**, this starts a new search query.

To edit a recent search query

- From the **View results** page, choose **Evidence finder** from the breadcrumb navigation menu.

AWS Audit Manager > **Evidence finder** > View results

Filtered by **Assessment** **Date range** **Compliance check** **Service category** **Resource type**

View results (1/12) [Info](#)

- Choose **Filters and grouping** to expand the filter selection.

Evidence finder [Info](#)

Evidence finder quickly retrieves and groups the evidence that's relevant to your search. To get started, apply filters to narrow the scope of your search. Then, choose how you want to group the results.

▶ Filters and grouping
4 filters applied.

- Next, edit your filters or start a new search.

- To edit filters, adjust or remove the current filters and grouping selection.
- To start over, choose **Clear filters** and apply the filters and grouping selection of your choice.



- When you're done, choose **Search**.



Viewing results in evidence finder

After your search is finished, you can view the results that matched your search criteria.

Keep in mind that multiple resources might be assessed during evidence collection. As a result, evidence can include one or more related resources. In evidence finder, results are shown at the resource level, with one row for each resource. You can preview a summary of each resource without leaving the page.

After you review the search results, you can generate an assessment report that includes that evidence. You can also export your search results into a comma-separated values (CSV) file.

Important

We recommend that you keep evidence finder open until you finished exploring your search results. Your search results are discarded when you navigate away from the **View Results** table. If needed, you can [view your recent results](#) in the CloudTrail console at <https://console.aws.amazon.com/cloudtrail/>. Here, the results of your search queries are preserved for seven days. However, keep in mind that you can't generate an assessment report from your search results in the CloudTrail console.

On this page

- [Viewing the grouped results \(p. 94\)](#)
- [Viewing the search results \(p. 94\)](#)
 - [Manage your viewing preferences \(p. 95\)](#)
 - [Preview resource summaries \(p. 95\)](#)
 - [Generate an assessment report from your search results \(p. 96\)](#)
 - [Export your search results \(p. 96\)](#)

Viewing the grouped results

If you grouped your results, you can review the groupings before you dive deeper into the evidence.

Note

If you didn't group results, evidence finder doesn't display the **Group by results** table. Instead, you're taken directly to the **View results** table.

Use the **Group by results** table to learn the breadth of the matching evidence and how it's distributed across a specific dimension. Results are grouped by the value that you selected. For example, if you grouped by **Resource type**, the table shows a list of AWS resource types. The **Total evidence** column shows the number of matching results for each resource type.

The screenshot shows a table titled "Group by results (1/2) Info". The table has two columns: "Resource type" and "Total evidence". There is one row visible, showing "AWS::S3::Bucket" in the "Resource type" column and "21" in the "Total evidence" column. A yellow box highlights the "Get results" button in the top right corner of the table header area.

Resource type	Total evidence
AWS::S3::Bucket	21

To get the results for a group

1. From the **Group by results** table, select the row for the results that you want to get.
2. Choose **Get results**. This starts a new search query, and redirects you to the **View results** table where you can see the results for that group.

Viewing the search results

The **View results** table displays your search results. From here, you can take the following actions:

- [Manage your viewing preferences \(p. 95\)](#)
- [Preview resource summaries \(p. 95\)](#)
- [Generate an assessment report from your search results \(p. 96\)](#)
- [Export your search results \(p. 96\)](#)

Manage your viewing preferences

Your viewing preferences control what you see on the results page.

To manage your viewing preferences

1. Choose the settings icon (#) at the top of the **View results** table.
2. Review and change the following settings as needed:
 - a. **Select visible table columns** – Use the toggle option to change which columns are displayed.
 - b. **Page size** – Select a radio button to specify how many results are shown on each page.
 - c. **Wrap text** – Select the check box to wrap long lines of text for better readability.
3. Choose **Confirm** to save your preferences.

Preview resource summaries

You can preview the related resources for the evidence that matched your search query. This helps you determine if the search query returned the intended results, or if you need to adjust your filters and re-run the search query.

Keep in mind that evidence can have one or more related resources. Evidence finder shows results at the resource level (with one row for each resource).

Note

Evidence finder returns results for automated and manual evidence. However, you can only preview resource summaries for automated evidence. This is because Audit Manager doesn't perform resource assessments for manual evidence, and as a result, no resource summary is available.

To see details about manual evidence, choose the evidence name to open the evidence details page. If you generate an assessment report from your evidence finder results, the manual evidence details are included in the assessment report.

To preview resource summaries

1. Select the radio button next to a result. This opens a resource summary panel on the current page.
2. (Optional) To see the full details of the related evidence, choose the evidence name.
3. (Optional) Use the horizontal lines (=) to drag and resize the resource summary pane.
4. Choose (x) to close the resource summary pane.

Evidence	Resource ARN	Resource compliance	Date and time
22615e944-a8b2-4cb0-85e4-d853ea94347b	arn:aws:iam:us-west1:XXXXXXXXXX:policyName	⚠ Non-compliant	August 10, 2022, 7:30 (UTC+00:00)
99615e944-a8b2-4cb0-85e4-d853ea94350d	arn:aws:cloudtrail:us-west-XXXXXXXXXX:trail/AWSOrganizationMaster	🟢 Compliant	August 10, 2022, 7:30 (UTC+00:00)
99615e944-a8b2-4cb0-85e4-d853ea94350d	arn:aws:cloudtrail:us-west-XXXXXXXXXX:trail/	🟢 Compliant	August 10, 2022, 7:30 (UTC+00:00)
99615e944-a8b2-4cb0-85e4-d853ea94350d			
Resource summary			
Resource ARN arn:aws:iam:us-west1:XXXXXXXXXX:policyName	Data source type AWS Config	Assessment PCI DSS V3.2.1	Control domain Identity and access management
Resource Type AWS:S3:Bucket	Data source mapping S3_BUCKET_PUBLIC_READ_PROHIBITED	Account ID XXXXXXXXXX	Control 7.2.1 Confirm that access control systems are in place on all system components.
Resource compliance ⚠ Non-compliant			
Date and time August 10, 2022, 7:30 (UTC+00:00)			

Generate an assessment report from your search results

After you're satisfied with the search results, generate an assessment report.

To generate an assessment report from your search results

1. At the top of the **View results** table, choose **Generate assessment report**.
 2. Enter a name and a description for your assessment report, and review the assessment report details.
 3. Choose **Generate assessment report**.

It takes a few minutes for your assessment report to be generated. You can navigate away from evidence finder while this happens, and a green success notification will confirm when the report is ready. You can then go to the Audit Manager download center and [download your assessment report](#).

Note

Audit Manager generates a one-time report using only the evidence from the search results. This report doesn't include any evidence that was manually [added to a report from the assessment page](#).

Limits apply to how much evidence can be included in an assessment report. For more information, see [Troubleshooting evidence finder](#).

Export your search results

You might need a portable version of your evidence finder search results. If this is the case, you can export your search results into a CSV file.

After you export your search results, the CSV file is available in the Audit Manager download center for seven days. A copy of the CSV file is also delivered to your preferred S3 bucket, which is known as an *export destination*. Your CSV file remains available in this bucket until you delete that file.

Audit Manager uses [CloudTrail Lake](#) functionality to export and deliver CSV files from evidence finder. The following factors define how the CSV export process works:

- All of your search results are included in the CSV file. If you want to include only specific search results, we recommend that you [edit your search filters](#). This way, you can narrow down your results to target only the evidence that you want to export.
- CSV files are exported in compressed GZIP format. The default CSV file name is `queryID/result.csv.gz`, where `queryID` is the ID of your search query.
- The maximum file size for a CSV export is 1 TB. If you're exporting over 1 TB of data, your results are split into more than one file. Each CSV file is named `result_number.csv.gz`. The number of CSV files that you get depends on the total size of your search results. For example, exporting 2 TB of data provides you with two query result files: `result_1.csv.gz` and `result_2.csv.gz`.
- In addition to the CSV file, a JSON sign file is delivered to your S3 bucket. This file acts as a checksum to verify that the information within the CSV file is accurate. To learn more, see [CloudTrail sign file structure](#) in the *AWS CloudTrail Developer Guide*. To determine whether the query results were modified, deleted, or unchanged after they were delivered, you can use the CloudTrail query results integrity validation. For instructions, see [Validate saved query results](#) in the *AWS CloudTrail Developer Guide*.

Note

Manual evidence text responses are not currently included in evidence finder previews or CSV exports. To see text response data, choose the manual evidence name in your evidence finder results to open the evidence details page. If you need to view text response data outside of the Audit Manager console, we recommend that you generate an assessment report from your evidence finder results. All manual evidence details, including text responses, are included in assessment reports.

Exporting your results for the first time

Follow these steps to export your search results for the first time. This procedure gives you the option to specify a default export destination for all of your future exports. If you don't want to save a default export destination right now, you can do so later by [updating your export destination settings](#).

Important

Before you start, make sure that you have an S3 bucket available to use as your export destination. You can use one of your existing S3 buckets, or you can [create a new bucket in Amazon S3](#). In addition, your S3 bucket must have the required permissions policy to allow CloudTrail to write the export files to it. More specifically, the bucket policy must include an `s3:PutObject` action and the bucket ARN, and list CloudTrail as the service principal. We provide an [example permission policy](#) that you can use. For instructions on how to attach this policy to your S3 bucket, see [Adding a bucket policy by using the Amazon S3 console](#).

For more tips, see [configuration tips for your export destination](#). If you encounter any issues when exporting a CSV file, see [Troubleshooting evidence finder CSV exports](#).

To export your search results (first-run experience)

1. At the top of the **View results** table, choose **Export CSV**.
2. Specify the S3 bucket that you want to export your file to.
 - Choose **Browse S3** to select from your list of buckets.
 - Alternatively, you can enter the bucket URI in this format: `s3://bucketname/prefix`

Tip

To keep your destination bucket organized, you can create an optional folder for your CSV exports. To do so, append a slash (/) and a prefix to the value in the **Resource URI** box (for example, `/evidenceFinderExports`). Audit Manager then includes this prefix when it

adds the CSV file to the bucket, and Amazon S3 generates the path specified by the prefix. For more information about prefixes in Amazon S3, see [Organizing objects in the Amazon S3 console](#) in the *Amazon Simple Storage Service User Guide*.

3. (Optional) If you don't want to save this bucket as your default export destination, clear the check box that says **Save this bucket as the default export destination in my evidence finder settings**.
4. Choose **Export**.

Exporting your results after you've saved an export destination

After you've saved a default S3 bucket as your default export destination, you can follow these steps moving forward.

To export your search results (after you saved a default export destination)

1. At the top of the **View results** table, choose **Export CSV**.
2. In the prompt that appears, review the default S3 bucket where your exported file will be saved.
 - a. (Optional) To continue using this bucket and hide this message moving forward, check the **Don't remind me again** box.
 - b. (Optional) To change this bucket, follow the procedure to [update your export destination settings](#).
3. Choose **Confirm**.

Depending on how much data you're exporting, the export process can take a few minutes to complete. You can navigate away from evidence finder while the export is in progress. When you navigate away from evidence finder, your search is stopped and your search results are discarded in the console. However, the CSV export process continues in the background. The CSV file will contain the complete set of search results that matched your query.

Viewing your results after you've exported them

To find your CSV file and check its status, go to the Audit Manager [download center](#). When the exported file is ready, you can [download your CSV file](#) from the download center.

You can also find and download the CSV file from your export destination S3 bucket.

To find your CSV file and sign file in the Amazon S3 console

1. Open the [Amazon S3 console](#).
2. Choose the export destination bucket that you specified when you exported your CSV file.
3. Navigate through the object hierarchy until you find the CSV file and the sign file. The CSV file has a .csv.gz extension and the sign file has a .json extension.

You will navigate through an object hierarchy that is similar to the following example, but with a different export destination bucket name, account ID, date, and query ID.

```
All Buckets
  Export_Destination_Bucket_Name
    AWSLogs
      Account_ID;
        CloudTrail-Lake
          Query
            YYYY
              MM
```

DD
Query_ID

Filter and grouping options

This page describes the filter and grouping options that are available in evidence finder.

On this page

- [Filter reference \(p. 99\)](#)
- [Grouping reference \(p. 102\)](#)

Filter reference

You can use the following filters to find evidence that matches specific criteria, such as an assessment, control, or AWS service.

Topics

- [Required filters \(p. 99\)](#)
- [Additional filters \(optional\) \(p. 100\)](#)
- [Combining filters \(p. 101\)](#)

Required filters

Use these filters to get started with a high-level overview of the evidence in an assessment.

Filter name	Description	Notes
Assessment	Returns evidence for a specific assessment.	You can filter by one assessment only.
Date range	Returns evidence for a specific time period.	Either, you can use a <i>Relative range</i> to define a range that's relative to today's date (for example, Last 30 days). Or, you can use an <i>Absolute range</i> to specify a specific date range (for example, June 27th – July 4th).
Resource compliance	Returns resources with a specific compliance check evaluation.	Audit Manager collects compliance check evidence for controls that use AWS Config and Security Hub as a data source type. Multiple resources might be assessed during evidence collection. As a result, a single piece of compliance check evidence can include one or more resources. You can use this filter to explore compliance status at the resource level. You can choose one or more of the following options: <ul style="list-style-type: none">• Non-compliant – This filter finds resources with compliance check issues. This happens if Security Hub reports a <i>Fail</i> result, or if AWS Config reports a <i>Non-compliant</i> result.

Filter name	Description	Notes
		<ul style="list-style-type: none"> Compliant – This filter finds resources that don't have compliance check issues. This happens if Security Hub reports a <i>Pass</i> result, or if AWS Config reports a <i>Compliant</i> result. Inconclusive – This filter finds resources for which a compliance check isn't available or applicable. This happens if a resource uses AWS Config or Security Hub as the underlying data source type, but those services aren't enabled. This also happens if the resource uses an underlying data source type that doesn't support compliance checks (such as manual evidence, AWS API calls, or CloudTrail).

Additional filters (optional)

Use these filters to narrow the scope of your search query. For example, use **Service** to see all evidence that's related to Amazon S3. Use **Resource type** to focus just on S3 buckets. Or, use **Resource ARN** to target a specific S3 bucket.

You can create additional filters using one or more of the following criteria.

Criteria name	Description	When to use this criteria
Account ID	Drill down by AWS account.	Use this criteria to find evidence that's related to a specific AWS account.
Control	Drill down by control name.	Use this criteria to find evidence that's related to a specific control.
Control domain	Drill down by control domain.	<p>Use this criteria to focus on a specific subject area as you prepare for an audit. You can filter by control domain if you're querying an assessment that was created from a standard framework.</p> <p>Examples of control domains include identity and access management, logging and monitoring, and network management.</p>
Data source type	Drill down by the type of data source.	<p>Use this criteria to focus on a specific data source.</p> <p>Set the value to Manual to find evidence that you uploaded manually. Otherwise, you can filter automated evidence based on where it came from (for example, AWS Config, CloudTrail, Security Hub, or AWS API calls).</p>
Event name	Drill down by event name.	<p>Use this criteria to focus on a specific event that the evidence is related to. An event is a record of an activity in an AWS account.</p> <p>For example, you can search for the name of an API call, such as the <code>IAM AttachRolePolicy</code> operation that's used to configure permissions. Or, search for a CloudTrail keyword, such as the <code>ConsoleLogin</code> event that's logged by CloudTrail when a user signs in to your account.</p>

Criteria name	Description	When to use this criteria
Resource ARN	Drill down by Amazon Resource Name (ARN).	Use this criteria to find evidence that's related to a specific AWS resource.
Resource type	Drill down by resource type.	Use this criteria to focus on the type of resource that's being assessed, such as an Amazon EC2 instance or an S3 bucket.
Service	Drill down by AWS service name.	Use this criteria to find evidence that's related to a specific AWS service, such as Amazon EC2, Amazon S3, or AWS Config.
Service category	Drill down by AWS service category.	Use this criteria to focus on a specific category of AWS service. Examples include security, identity and compliance, database, and storage.

Combining filters

Criteria behavior

When you specify more than one criteria, Audit Manager applies the AND operator to your selections. This means that all of the criteria are grouped into a single query, and the results must match all of the combined criteria.

Example

In the following filter setup, evidence finder returns non-compliant resources from the last 7 days for the assessment that's called **MySOC2Assessment**. Additionally, the results relate to both an IAM policy and the specified control.

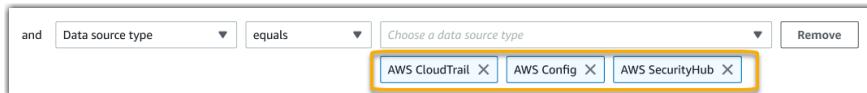
The screenshot shows the AWS Audit Manager Evidence Finder interface. At the top, the assessment is set to "MySOC2Assessment" and the date range is "Last 7 days". Below this, under "Resource compliance info", the "Non-compliant" checkbox is checked. In the "Additional filters - optional" section, there are two criteria defined. The first criterion is "Control equals 7.2.1 Confirm that access control systems are in place on all system components.", with the entire condition highlighted by a yellow box. The second criterion is "Resource type contains AWS::IAM::Policy". At the bottom left, there is a button labeled "Add criteria".

Criteria value behavior

When you specify more than one criteria value, the values are linked with an OR operator. Evidence finder returns results that match any of these criteria values.

Example

In the following filter setup, evidence finder returns search results that come from either AWS CloudTrail, AWS Config, or AWS Security Hub.



Grouping reference

You can group your search results for quicker navigation. Grouping shows you the breadth of your search results, and how they're distributed across a specific dimension.

You can use any of the following group by values.

Group by	Description
Account ID	Group results by AWS account.
Control	Group results by control name.
Control domain	Group results by control domain.
Data source type	Group results by the type of data source where the evidence came from.
Event name	Group results by an event name.
Resource ARN	Group results by Amazon Resource Name (ARN).
Resource type	Group results by resource type.
Service	Group results by AWS service name.
Service category	Group results by AWS service category.

Example use cases

Evidence finder can help you with several use cases. This page provides some examples and suggests the search filters that you can use in each scenario.

Topics

- [Use case 1: Find non-compliant evidence and organize delegations \(p. 102\)](#)
- [Use case 2: Identify compliant evidence \(p. 103\)](#)
- [Use case 3: Perform a quick preview of evidence resources \(p. 104\)](#)

Use case 1: Find non-compliant evidence and organize delegations

This use case is ideal if you're a compliance officer, a data protection officer, or a GRC professional who oversees audit preparation.

As you monitor the compliance posture for your organization, you might rely on partner teams to help you remediate issues. You can use evidence finder to help you organize your work for your partner teams.

By applying filters, you can focus on evidence for one area at a time. Moreover, you can also stay aligned with the responsibilities and scope of each partner team that you work with. By performing a targeted search in this way, you can use the search results to identify what exactly needs remediating in each subject area. You can then delegate that non-compliant evidence to the corresponding partner team for remediation.

For this workflow, follow the steps to [search for evidence](#). Use the following filters to find non-compliant evidence.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Non-compliant
```

Next, apply additional filters for the area that you're focusing on. For example, use the **Service category** filter to find non-compliant resources that are related to IAM. Then, share those results with the team that owns IAM resources for your organization. Or, if you're querying an assessment that was created from a standard framework, you can use the **Control domain** filter to find non-compliant evidence that's related to the identity and access management domain.

```
Control domain | <domain that you're focusing on>
or
Service category | <AWS service category that you're focusing on>
```

After you find the evidence that you need, follow the steps to [generate an assessment report from the search results](#). You can share this report with your partner team, who can use it as a remediation checklist.

Use case 2: Identify compliant evidence

This use case is ideal if you work in SecOps, IT/DevOps, or another role that owns and remediates cloud assets.

As part of an audit, you might be asked to remediate issues with the resources that you own. After you do this work, you can use evidence finder to validate that your resources are compliant.

For this workflow, follow the steps to [search for evidence](#). Use the following filters to find compliant evidence.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Compliant
```

Next, apply additional filters to show only the evidence that you're responsible for. Depending on your ownership scope, make the search as targeted as needed. The following filter examples are ordered from broadest to most precise. Choose the appropriate options for you, and replace the *<placeholder text>* with your own values.

```
Control domain | <a subject area that you're responsible for>
Service category | <a category of AWS services that you own>
Service | <a specific AWS service that you own>
Resource type | <a collection of resources that you own>
Resource ARN | <a specific resource that you own>
```

If you're responsible for multiple instances of the same criteria (for example, you own multiple AWS services), you can [group your results](#) by that value. This provides you with the total evidence matches for each AWS service. You can then get the results for the services that you own.

Use case 3: Perform a quick preview of evidence resources

This use case is ideal for all Audit Manager customers.

Previously, it was time consuming to review individual evidence details. If you wanted to preview evidence, you had to go directly to that assessment, then navigate through deeply nested evidence folders. Now, evidence finder provides a convenient way to preview this information. For each evidence item that matches your search query, you can preview the individual resources for that evidence.

To get started, follow the steps to [search for evidence](#). Then, select the radio button next to a result to see a resource summary in the current page. You can preview each individual resource that relates to an evidence item. To see the full evidence details for any resource, choose the evidence name. For more information, see [Preview resource summaries](#).

Evidence	Resource ARN	Resource compliance	Date and time
22615e944-a8b2-4cb0-85e4-d853ea94347b	arn:aws:iam:us-west-1: REDACTED :policyName	⚠ Non-compliant	August 10, 2022, 7:30 (UTC+00:00)
99615e944-a8b2-4cb0-85e4-d853ea94350d	arn:aws:cloudtrail:us-west-1: REDACTED :trail/AWSOrganizationMaster	🟢 Compliant	August 10, 2022, 7:30 (UTC+00:00)
99615e944-a8b2-4cb0-85e4-d853ea94350d	arn:aws:cloudtrail:us-west-1: REDACTED :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: REDACTED :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)		

Audit Manager download center

The download center is where you can find and manage all of your downloadable Audit Manager files. When you generate an assessment report or export search results from evidence finder, the files appear in the download center.

Topics

- [Browsing the download center \(p. 105\)](#)
- [Downloading a file \(p. 106\)](#)
- [Deleting a file \(p. 106\)](#)

Browsing the download center

To visit the download center, open the Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>, and then choose **Download center** in the left navigation pane.

You can switch between the following tabs to browse your files by category.

Assessment reports tab

This tab shows all the assessment reports that you've generated. Assessment reports remain available in the download center until you delete them.

To see the latest status of your assessment report, choose the refresh icon (#) to reload the table. Each row in the assessment reports table shows the name of the report, its creation date, and one of the following statuses:

- **In progress** – Audit Manager is generating the assessment report.
- **Ready** – The assessment report is available for you to download.
- **Error** – The assessment report failed to generate. In this case, Audit Manager displays a message that describes the error. For information about how to resolve these errors, see [Troubleshooting assessment reports](#).

Exports tab

This tab shows all the evidence finder search results that you exported in the last seven days. CSV files are removed from the download center after seven days, but they remain available in your [export destination](#) S3 bucket. For instructions on how to find an evidence finder CSV export in your S3 destination bucket, see [Viewing your results after you've exported them \(p. 98\)](#).

To see the latest status of your CSV exports, choose the refresh icon (#) to reload the table. Each row in the exports table shows the file name, its export date, and one of the following statuses:

- **In progress** – Audit Manager is preparing the CSV file.
- **Ready** – The export succeeded and the file is available for you to download.
- **Error** – The export failed. In this case, Audit Manager displays a message that describes the error. For information about how to resolve these errors, see [Troubleshooting evidence finder CSV export issues](#).

Note

Keep in mind that the exports tab might also display CSV files for queries that you ran directly in AWS CloudTrail Lake. This includes queries made in the CloudTrail console or using the CloudTrail API. CloudTrail exports appear on this tab if you queried the Audit Manager event data store, and you chose to save the results to Amazon S3.

Downloading a file

Follow these steps to download a file from the download center.

To download a file

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the left navigation pane, choose **Download center**.
3. Choose either the **Assessment reports** tab or the **Exports** tab.
4. Select the file that you want to download, and choose **Download**.

For instructions on how to download a file from your S3 destination bucket, see [Downloading an object](#) in the *Amazon Simple Storage Service (Amazon S3) User Guide*.

Deleting a file

Follow these steps to delete any assessment reports that you no longer need in the download center.

Note

Deleting CSV exports from the download center isn't currently supported. CSV exports are automatically removed from the download center after seven days.

To delete an assessment report

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the left navigation pane, choose **Download center**.
3. Choose the **Assessment reports** tab.
4. Select the assessment report that you want to delete, and choose **Delete**.

If you want to delete an assessment report or a CSV export from your S3 destination bucket, we recommend that you complete this task directly in Amazon S3. For instructions, see [Deleting Amazon S3 objects](#) in the *Amazon Simple Storage Service (Amazon S3) User Guide*.

Framework library

You can access and manage frameworks from the *framework library* in AWS Audit Manager.

A framework determines which controls are tested in an environment over a period of time. It defines the controls and their data source mappings for a given compliance standard or regulation. It's also used to structure and automate Audit Manager assessments. You can use frameworks as a starting point to audit your AWS service usage and start automating evidence collection.

The framework library contains a catalog of both standard and custom frameworks.

- **Standard frameworks** are prebuilt frameworks that AWS provides. These frameworks are based on AWS best practices for different compliance standards and regulations. These include GDPR and HIPAA. Standard frameworks include controls that are organized into control sets that are based on the compliance standard or regulation that the framework supports.

You can view the contents of standard frameworks, but you can't edit or delete them. However, you can customize any standard framework to create a new one to meet your specific requirements.

- **Custom frameworks** are customized frameworks that you own. You can create a custom framework from scratch, or by customizing an existing framework. You can use custom frameworks to organize controls into control sets in a way that meets your specific requirements. To learn more about how to manage controls, see [Control library \(p. 200\)](#).

You can create an assessment from a standard framework or a custom framework. To learn about how to create and manage assessments, see [Assessments in AWS Audit Manager \(p. 50\)](#).

Note

AWS Audit Manager assists in collecting evidence that's relevant for verifying compliance with specific compliance standards and regulations. However, it doesn't assess your compliance itself. The evidence that's collected through AWS Audit Manager therefore might not include all the information about your AWS usage that's needed for audits. AWS Audit Manager isn't a substitute for legal counsel or compliance experts.

This section describes how you can create and manage custom frameworks in Audit Manager.

Topics

- [Accessing the available frameworks in AWS Audit Manager \(p. 107\)](#)
- [Viewing the details of a framework \(p. 108\)](#)
- [Creating a custom framework \(p. 110\)](#)
- [Editing a custom framework \(p. 114\)](#)
- [Deleting a custom framework \(p. 115\)](#)
- [Sharing a custom framework \(p. 116\)](#)
- [Supported frameworks in AWS Audit Manager \(p. 127\)](#)

Accessing the available frameworks in AWS Audit Manager

You can view all available frameworks on the **Framework library** page in the Audit Manager console. From here, you can also [create an assessment from a framework](#), [create a custom framework](#), or [customize an existing framework](#).

You can also view all available frameworks using the Audit Manager API or the AWS Command Line Interface (AWS CLI).

Audit Manager console

To view available frameworks (console)

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the left navigation pane, choose **Framework library**.
3. Choose the **Standard frameworks** tab or the **Custom frameworks** tab to browse the available standard and custom frameworks.
4. Choose any framework name to view the details of that framework.

AWS CLI

To view available frameworks (AWS CLI)

To view frameworks in Audit Manager, use the [list-assessment-frameworks](#) command and specify a `--framework-type`. Either, you can retrieve a list of standard frameworks. Or, you can retrieve a list of custom frameworks.

```
aws auditmanager list-assessment-frameworks --framework-type Standard
```

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

Audit Manager API

To view available frameworks (API)

Use the [ListAssessmentFrameworks](#) operation and specify a [frameworkType](#). Either, you can return a list of standard frameworks. Or, you can return a list of custom frameworks.

For more information, choose either of the previous links to read more in the *AWS Audit Manager API Reference*. This includes information about how to use the ListAssessmentFrameworks operation and parameters in one of the language-specific AWS SDKs.

Viewing the details of a framework

You can review the details of a framework using the Audit Manager console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI).

Audit Manager console

To view framework details (console)

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the left navigation pane, choose **Framework library** to see a list of available frameworks.
3. Choose the **Standard frameworks** tab or the **Custom frameworks** tab to browse the available frameworks.
4. Choose the name of the framework to open it.

When you open a framework, a **Framework details** page is displayed. The sections of this page and their contents are described as follows.

Framework details section

This section provides an overview of the framework. It includes the following information:

- **Framework name** – The name of the framework.
- **Compliance type** – The compliance standard or regulation that the framework supports.
- **Description** – A description of the framework, if one was provided.
- **Framework type** – Specifies whether the framework is a standard framework or a custom framework.
- **Control sets** – The number of control sets that are associated with the framework.
- **Controls** – The total number of controls in the framework.
- **Control sources** – The number of control data sources where Audit Manager collects evidence from.
- **Tags** – The tags that are associated with the framework.

If you're viewing a custom framework, the following details are also displayed:

- **Created by** – The account that created the custom framework.
- **Date created** – The date that the custom framework was created.
- **Last updated** – The date when this framework was last edited.

Controls tab

This tab lists the controls in the framework, grouped by control set. It includes the following information:

- **Controls grouped by control set** – Choose the tree view icon to see the controls that belong to each control set.
- **Type** – Specifies whether the control is a standard control or a custom control.
- **Data source** – Specifies the data source where Audit Manager collects evidence from for that control.

Tags tab

This tab lists the tags that are associated with the framework. It includes the following information:

- **Key** – The tag key (for example, a compliance standard, regulation, or category).
- **Value** – The tag value.

AWS CLI

To view framework details (AWS CLI)

1. To identify the framework that you want to review, run the [list-assessment-frameworks](#) command and specify a --framework-type. Either, you can retrieve a list of standard frameworks. Or, you can retrieve a list of custom frameworks.

In the following example, replace the *placeholder text* with either Custom or Standard.

```
aws auditmanager list-assessment-frameworks --framework-type Custom/Standard
```

The response returns a list of frameworks. Find the framework that you want to review, and take note of the framework ID and Amazon Resource Name (ARN).

2. To get the framework details, run the [get-assessment-framework](#) command and specify the --framework-id.

In the following example, replace the *placeholder text* with your own information.

```
aws auditmanager get-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-  
EXAMPLE11111
```

The framework details are returned in JSON format. To understand this data, see [get-assessment-framework Output](#) in the *AWS CLI Command Reference*.

3. To see the tags for a framework, use the [list-tags-for-resource](#) command and specify the --resource-arn for the framework.

In the following example, replace the *placeholder text* with your own information:

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-  
east-1:111122223333:assessmentFramework/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

For more information about tags in Audit Manager, see [Tagging AWS Audit Manager resources](#).

Audit Manager API

To view framework details (API)

1. To identify the framework that you want to review, use the [ListAssessmentFrameworks](#) operation and specify a [frameworkType](#). Either, you can return a list of standard frameworks. Or, you can return a list of custom frameworks.

From the response, find the framework that you want to review and note the framework ID and Amazon Resource Name (ARN).

2. To get the framework details, use the [GetAssessmentFramework](#) operation. In the request, specify the [frameworkId](#) that you got from step 1.

The framework details are returned in JSON format. To understand this data, see [GetAssessmentFramework Response Elements](#) in the *AWS Audit Manager API Reference*.

3. To see tags for the framework, use the [ListTagsForResource](#) operation. In the request, specify the framework [resourceArn](#) that you got from step 1.

For more information about tags in Audit Manager, see [Tagging AWS Audit Manager resources](#).

For more information about these API operations, choose any of the previous links to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Creating a custom framework

You can access and manage frameworks from the framework library in AWS Audit Manager. You can create custom frameworks to organize controls into control sets in a way that meets your specific requirements.

There are two ways to create a custom framework. Either you can customize an existing framework, or you can create a new framework from scratch.

Topics

- [Creating a new custom framework from scratch \(p. 111\)](#)
- [Customizing an existing framework \(p. 112\)](#)

Creating a new custom framework from scratch

You can use custom frameworks in AWS Audit Manager to organize controls into control sets in a way that meets your specific requirements. You can create a new custom framework from scratch in the framework library by following these steps.

Topics

- [Step 1: Specify framework details \(p. 111\)](#)
- [Step 2: Specify the controls in the control sets \(p. 111\)](#)
- [Step 3: Review and create the framework \(p. 112\)](#)
- [What can I do next? \(p. 112\)](#)

Step 1: Specify framework details

Start by specifying the controls that you want to include in your custom framework.

To specify framework details

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the left navigation pane, choose **Framework library**, and choose **Create custom framework**.
3. Under **Framework detail**, enter a name, a compliance standard or regulation (optional), and a description for your framework (also optional). Enter a compliance standard or regulation keyword such as *PCI_DSS* or *GDPR* so that you can use this keyword to search for your framework.
4. Under **Tags**, choose **Add new tag** to associate a tag with your framework. You can specify a key and a value for each tag. The tag key is mandatory. You can use it as search criteria when searching for this framework in the Framework library. For more information about tags in AWS Audit Manager, see [Tagging AWS Audit Manager resources \(p. 367\)](#).
5. Choose **Next**.

Step 2: Specify the controls in the control sets

Next, you specify which controls you want add to your framework and how you want to organize them. Start by adding control sets to the framework, and then add controls to the control set.

Note

When you use the AWS Audit Manager console to create a custom framework, you can add up to 10 control sets for each framework.

When you use the Audit Manager API to create a custom framework, you can create more than 10 control sets. To add more control sets than the console currently allows, use the [CreateAssessmentFramework](#) API that Audit Manager provides.

To specify the controls in the control sets

1. Under **Control set name**, enter a name for your control set.
2. Under **Add a new control to the control set**, **Select control type**, use the dropdown list to select one of the two control types: **Standard controls** or **Custom controls**. Standard controls are provided by Audit Manager, and custom controls are the ones that you create.
3. Based on the option that you selected in the previous step, a list of standard controls or custom controls is displayed. You can browse the list, or search by entering the control name, compliance, or tag. Select one or more controls and choose **Add to control set** to add them to the control set.
4. In the pop-up window that appears, choose **Add to control set** to confirm your addition.

5. Under **Review the selected controls in the control set**, review the controls that appear in the **Selected controls** list. To add more controls to a control set, repeat steps 2–4. You can remove unwanted controls from the control set by selecting one or more controls and choosing **Remove control**.
6. To add a new control set to the framework, choose **Add control set** at the bottom of the page. You can remove unwanted control sets by choosing **Remove control set**.
7. After you finish adding control sets and controls, choose **Next**.

Step 3: Review and create the framework

Review the information for your framework. To change the information for a step, choose **Edit**.

When you're finished, choose **Create custom framework**.

What can I do next?

After you create your new custom framework, you can create an assessment from your framework. For more information, see [Creating an assessment \(p. 50\)](#).

You can also create a custom framework using an existing framework. For more information, see [Customizing an existing framework \(p. 112\)](#).

For instructions on how to edit your custom framework, see [Editing a custom framework \(p. 114\)](#).

Customizing an existing framework

With custom frameworks in AWS Audit Manager, you can organize controls into control sets in a way that meets your specific requirements. Instead of creating a custom framework from scratch, you can use an existing framework as a starting point and customize it. When you do this, the existing framework remains in the framework library, and a new custom framework is created with your customized settings.

You can select any existing framework to customize. It can be either a standard framework or a custom framework.

In the framework library, from the **Create custom framework** dropdown list, choose **Customize existing framework**. Use the following steps to customize the framework.

Topics

- [Step 1: Specify framework details \(p. 112\)](#)
- [Step 2: Specify controls to add to control sets \(p. 113\)](#)
- [Step 3: Review and create the framework \(p. 113\)](#)
- [What can I do next? \(p. 113\)](#)

Step 1: Specify framework details

All framework details, except tags, are carried over from the original framework. Review and modify these details as needed.

To specify framework details

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the left navigation pane, choose **Framework library**.
3. Choose the framework you want to customize, and from the **Create custom framework** dropdown list, choose **Customize existing framework**.

4. In the pop-up window that appears, enter a name for the new custom framework and choose **Customize**.
5. Under **Framework detail**, review the name, compliance type, and description for your framework, and modify them as needed. The compliance type should indicate the compliance standard or the regulation that's associated with your framework. You can use this keyword to search for your framework.
6. Under **Tags**, choose **Add new tag** to associate a tag with your framework. You can specify a key and a value for each tag. The tag key is mandatory and can be used as a search criteria when you search for this framework in the Framework library. For more information about tags in AWS Audit Manager, see [Tagging AWS Audit Manager resources \(p. 367\)](#).
7. Choose **Next**.

Step 2: Specify controls to add to control sets

The control sets are carried over from the original framework. Customize the current configuration by adding more controls or removing existing controls as needed.

Note

When you use the AWS Audit Manager console to customize a framework, you can add up to 10 control sets for each framework.

When you use the Audit Manager API to create a custom framework, you can add more than 10 control sets. To add more control sets than the console currently allows, use the [CreateAssessmentFramework](#) API that Audit Manager provides.

To specify controls in the control set

1. Under **Control set name**, customize the name of the control set as needed.
2. Under **Add a new control to the control set**, add a new control by using the dropdown list to select one of the two control types: **Standard controls** or **Custom controls**.
3. Based on the option that you selected in the previous step, a list of standard controls or custom controls is displayed. You can browse this list, or search by entering the control name, compliance, or tags to locate the controls that you want to add. Select one or more controls and choose **Add to control set** to add to this control set.
4. In the pop-up window that appears, choose **Add to control set** to confirm your addition.
5. Under **Review the selected controls in the control set**, review the controls that appear in the **Selected controls** list. To add more controls to a control set, repeat steps 2–4. You can remove unwanted controls from the control set by selecting one or more controls and choosing **Remove control**.
6. To add a new control set to the framework, choose **Add control set** at the bottom of the page. You can remove unwanted control sets by choosing **Remove control set**.
7. After you finish adding control sets and controls, choose **Next**.

Step 3: Review and create the framework

Review the information for your framework. To change the information for a step, choose **Edit**.

When you're finished, choose **Create custom framework**.

What can I do next?

After you create your new custom framework, you can create an assessment from your framework. For more information, see [Creating an assessment \(p. 50\)](#).

For instructions on how to edit your custom framework, see [Editing a custom framework \(p. 114\)](#).

Editing a custom framework

You can use custom frameworks in AWS Audit Manager to organize controls into control sets to meet your specific needs. You can use the framework library to find and edit a custom framework by following these steps.

Topics

- [Step 1: Edit framework details \(p. 114\)](#)
- [Step 2: Edit the controls in the control set \(p. 114\)](#)
- [Step 3: Review and update the framework \(p. 115\)](#)

Step 1: Edit framework details

Start by reviewing and editing the existing framework details.

To edit framework details

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the left navigation pane, choose **Framework library** and then choose the **Custom frameworks** tab.
3. Select the framework that you want to edit, choose **Actions**, and then choose **Edit**.
 - Alternatively, you can open a custom framework and choose **Actions**, **Edit** at the top right of the assessment summary page.
4. Under **Framework detail**, review the name, compliance type, and description for your framework, and make any necessary changes.
5. Choose **Next**.

Tip

To edit the tags for a framework, open the framework and choose the [framework tags tab](#). There you can view and edit the tags that are associated with the framework.

Step 2: Edit the controls in the control set

Next, review and edit the controls and control sets in the framework.

Note

When you use the AWS Audit Manager console to edit a custom framework, you can add up to 10 control sets for each framework.

When you use the Audit Manager API to edit a custom framework, you can add more than 10 control sets. To add more control sets than the console currently allows, use the [UpdateAssessmentFramework](#) API that Audit Manager provides.

To edit controls

1. Under **Control set name**, review and edit the name for your control set as needed.
2. Under **Add a new control to the control set**, you can add a control. Use the dropdown list to select one of the two control types: **Standard controls** or **Custom controls**.
3. Based on the option you selected in the previous step, a table list of standard controls or custom controls is displayed. You can browse the list for control sets. Or, you can search by entering the control name, data source, or tags to locate the controls that you want to add. Select one or more controls and choose **Add to control set** to add to this control set.

4. In the pop-up window that appears, choose **Add to control set** to confirm your addition.
5. Under **Review the selected controls in the control set**, review and edit the controls that currently appear in the **Selected controls** list. To add more controls to a control set, repeat steps 2–4. Remove unwanted controls from the control set by selecting one or more controls and choosing **Remove control**.
6. To add a new control set to the framework, choose **Add control set** at the bottom of the page. Remove unwanted control sets by choosing **Remove control set**.
7. After you finish adding control sets and controls, choose **Next**.

Step 3. Review and update the framework

Review the information for your framework. To change the information for a step, choose **Edit**.

When you're finished, choose **Save changes**.

Deleting a custom framework

You can use the framework library to find and delete an unwanted custom framework. You can also delete custom frameworks using the Audit Manager API or the AWS Command Line Interface (AWS CLI).

Note

Deleting a custom framework doesn't affect any existing assessments that were created from the framework before it was deleted.

Audit Manager console

To delete a custom framework (console)

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the left navigation pane, choose **Framework library** and then choose the **Custom frameworks** tab.
3. Select the framework that you want to delete, choose **Actions**, and then choose **Delete**.
 - Alternatively, you can open a custom framework and choose **Actions**, **Delete** at the top right of the framework summary page.
4. In the pop-up window, choose **Delete** to confirm deletion.

AWS CLI

To delete a custom framework (AWS CLI)

1. First, identify the custom framework that you want to delete. To do this, run the [list-assessment-frameworks](#) command and specify the `--framework-type` as `Custom`.

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

The response returns a list of custom frameworks. Find the custom framework that you want to delete, and take note of the framework ID.

2. Next, run the [delete-assessment-framework](#) command and specify the `--framework-id` of the framework that you want to delete.

In the following example, replace the `placeholder text` with your own information.

```
aws auditmanager delete-assessment-framework --framework-id a1b2c3d4-5678-90ab-  
cdef-EXAMPLE11111
```

Audit Manager API

To delete a custom framework (API)

1. Use the [ListAssessmentFrameworks](#) operation and specify the [frameworkType](#) as Custom. From the response, find the custom framework that you want to delete, and take note of the framework ID.
2. Use the [DeleteAssessmentFramework](#) operation to delete the framework. In the request, use the [frameworkId](#) parameter to specify the framework that you want to delete.

For more information about these API operations, choose any of the previous links to read more in the [AWS Audit Manager API Reference](#). This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Sharing a custom framework

You can use the framework sharing feature of AWS Audit Manager to quickly replicate the custom frameworks that you create. You can share your custom frameworks with another AWS account, or replicate your frameworks into another AWS Region under your own account. The recipient can then access your custom framework and use it to create assessments. They can do this without having to repeat any of your configuration efforts for that framework.

To share a custom framework, you create a *share request*. The recipient of the share request then has 120 days to accept or decline the request. When they accept the share request, Audit Manager replicates the shared custom framework into their framework library. In addition to replicating the custom framework, Audit Manager also replicates any custom control sets and custom controls that are part of that framework. These custom controls are then added to the recipient's control library. Audit Manager doesn't replicate standard frameworks or controls. By default, these are available in all AWS accounts and Regions where Audit Manager is enabled.

The framework sharing feature is available on the paid tier only. However, there are no additional charges for sharing a custom framework or accepting a share request. To learn more about pricing for AWS Audit Manager, see the [AWS Audit Manager pricing page](#).

Important

You may not share a custom framework that is derived from a standard framework if the standard framework is designated as not eligible for sharing by AWS, unless you have obtained permission to do so from the owner of the standard framework. To see which standard frameworks are not eligible for sharing and learn more, see [Framework sharing eligibility](#).

The following sections of this guide describe the important things that you should know about framework sharing. They also provide instructions on how you can share your custom frameworks and respond to share requests.

Topics

- [Framework sharing concepts and terminology \(p. 117\)](#)
- [Sending a share request for a custom framework \(p. 120\)](#)
- [Responding to share requests \(p. 124\)](#)
- [Deleting share requests \(p. 127\)](#)

Tip

If you aren't familiar with Audit Manager custom frameworks and how to create them, you can learn more on the [Creating a custom framework](#) page of this guide.

Framework sharing concepts and terminology

If you learn about the following key concepts, you can get more out of the AWS Audit Manager custom framework sharing feature.

Sender

This is the creator of a share request and the AWS account where the custom framework exists. Senders can share custom frameworks with any AWS account. Or, they replicate a custom framework to any supported AWS Region under their own account.

Recipient

This is the consumer of the shared framework. Recipients can either accept or decline a share request from a sender.

Note

A recipient can be a delegated administrator account. However, you can't share custom frameworks with an AWS Organizations management account.

Framework eligibility

You can only share custom frameworks. By default, standard frameworks are already present in all AWS accounts and AWS Regions where AWS Audit Manager is enabled. In addition, the custom frameworks that you share must not contain sensitive data. This includes data found within the framework itself, its control sets, and any of the custom controls that are part of the custom framework.

Important

Some of the standard frameworks that are offered by AWS Audit Manager contain copyrighted material that's subject to license agreements. Custom frameworks might contain content that's derived from these frameworks. You may not share a custom framework that's derived from a standard framework if the standard framework is designated as not eligible for sharing by AWS, unless you have obtained permission to do so from the owner of the standard framework.

To learn which standard frameworks are eligible for sharing, refer to the following table.

Standard framework name	Custom versions eligible for sharing
Australian Cyber Security Centre (ACSC) Essential Eight	Yes
Australian Cyber Security Centre (ACSC) Information Security Manual	Yes
AWS Audit Manager Sample Framework	Yes
AWS Control Tower Guardrails	Yes
AWS generative AI best practices framework v1	Yes
AWS License Manager	Yes
AWS Foundational Security Best Practices	Yes
AWS Operational Best Practices	Yes

Standard framework name	Custom versions eligible for sharing
AWS Well-Architected Framework	Yes
Canadian Centre for Cyber Security - Medium	No
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.2.0, Level 1	No
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.2.0, Level 1 and 2	No
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0, Level 1	No
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0, Level 1 and 2	No
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4.0, Level 1	No
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4.0, Level 1 and 2	No
CIS Controls v7.1 IG1	Yes
CIS Controls v8 IG1	No
FedRAMP Moderate Baseline	Yes
GDPR	Yes
Gramm-Leach-Bliley Act (GLBA)	Yes
GxP 21 CFR Part 11	Yes
GxP EU Annex 11	Yes
HIPAA Security Rule 2003	Yes
HIPAA Final Omnibus Security Rule 2013	Yes
ISO/IEC 27001:2013 Annex A	No
NIST 800-53 (Rev. 5) Low-Moderate-High	Yes
NIST Cybersecurity Framework version 1.1	Yes
NIST SP 800-171 Rev. 2	Yes
PCI DSS	No
SOC 2	No

Share request

To share a custom framework, you create a *share request*. The share request specifies a recipient and notifies them that a custom framework is available. Recipients have 120 days to respond to a share request by accepting or declining. If no action is taken in 120 days, the share request expires and the recipient loses the ability to add the custom framework to their framework library. Senders and recipients can view and take action on share requests from the share requests page of the framework library.

Share request status

Share requests can have any of the following statuses.

- **Active** – This indicates a share request that was successfully sent to the recipient and is waiting for their response.
- **Expiring** – This indicates a share request that expires within the next 30 days.
- **Shared** – This indicates a share request that the recipient accepted.
- **Inactive** – This indicates a share request that was revoked, declined, or expired before the recipient took action.
- **Replicating** – This indicates an accepted share request that's being replicated to the recipient's framework library.
- **Failed** – This indicates a share request that wasn't successfully sent to the recipient.

Share request notifications

Audit Manager notifies recipients when they receive a share request. Both recipients and senders receive a notification when a share request is due to expire sometime in the next 30 days.

- For recipients, a blue notification dot appears next to received requests with an **Active** or **Expiring** status. The recipient can resolve the notification by accepting or declining the share request.
- For senders, a blue notification dot appears next to sent requests with an **Expiring** status. The notification is resolved when the recipient accepts or declines the request. Otherwise, it's resolved when the request expires. Additionally, the sender can resolve the notification by revoking the share request.

Sender ownership

Senders maintain full access over the custom frameworks that they share. They can cancel active share requests at any time by [revoking the share request](#) before it expires. However, after a recipient accepts a share request, the sender can no longer revoke the recipient's access to that custom framework. This is because when the recipient accepts the request, Audit Manager creates an independent copy of the custom framework in the recipient's framework library.

In addition to replicating the sender's custom framework, Audit Manager also replicates any custom control sets and custom controls that are part of that framework. However, Audit Manager doesn't replicate any tags that are attached to the custom framework.

Recipient ownership

Recipients have full access over the custom frameworks that they accept. When recipient accepts the request, Audit Manager replicates the custom framework to the custom frameworks tab of their framework library. Recipients can then manage the shared custom framework in the same way as any other custom framework. Recipients can share the custom frameworks that they receive from other senders. Recipients can't block senders from sending share requests.

Shared framework expiration

When a sender creates a share request, Audit Manager sets the request to expire after 120 days. Recipients can accept and gain access to the shared framework before the request expires. If a recipient doesn't accept during this time, the share request expires. After this point, a record of the expired share request remains in their history. Snapshots of expired shared frameworks are archived to an S3 bucket with a one-year TTL for audit purposes.

Senders can choose to [revoke a share request](#) at any time before it's due to expire.

Shared framework data storage and backup

When you create a share request, Audit Manager stores a snapshot of your custom framework in the US East (N. Virginia) AWS Region. Audit Manager also stores a backup of the same snapshot in the US West (Oregon) AWS Region.

Audit Manager deletes the snapshot and the backup snapshot when one of the following events occurs:

- The sender revokes the share request.
- The recipient declines the share request.
- The recipient encounters an error and doesn't successfully accept the share request.
- The share request expires before the recipient responds to the request.

When a sender [resends a share request](#), the snapshot is replaced with an updated version that corresponds with the latest version of the custom framework.

When a recipient accepts a share request, the snapshot is replicated into their AWS account under the AWS Region that was specified in the share request.

Shared framework versioning

When you share a custom framework, Audit Manager creates an independent copy of that framework in the specified AWS account and Region. This means that you should keep in mind the following points:

- The shared framework that a recipient accepts is a snapshot of the framework at the time of the share request creation. If you update the original custom framework after sending a share request, the request isn't automatically updated. To share the latest version of the updated framework, you can [resend the share request](#). The expiration date of this new snapshot is 120 days from the re-share date.
- When you share a custom framework with another AWS account and then delete it from your framework library, the shared custom framework remains in the recipient's framework library.
- When you share a custom framework to another AWS Region under your account and then delete that custom framework in the first AWS Region, the custom framework remains in the second Region.
- When you delete a shared custom framework after accepting it, any custom controls that were replicated as part of the custom framework remain in your control library.

Sending a share request for a custom framework

This tutorial describes how to share your custom frameworks across AWS accounts and AWS Regions.

When you share a custom framework, Audit Manager creates a snapshot of your framework and sends a share request to the recipient. The recipient has 120 days to accept the shared framework. When they accept, Audit Manager replicates the shared custom framework to their framework library in the specified AWS Region. If you want to replicate a custom framework to another Region under your own account, use the following tutorial and enter your own AWS account ID as the recipient account ID.

This tutorial covers the following steps:

1. [Select a framework to share](#) – Browse the framework library to find the custom framework that you want to share.
2. [Send a share request](#) – Specify a recipient and send them a share request for the custom framework.
3. [View sent requests](#) – View your share request history and check the status of your sent requests.
4. [\(Optional\) Revoke the share request](#) – Revoke the share request before it's due to expire.

Prerequisites

Before you start this tutorial, make sure that you first meet the following conditions:

- You're familiar with Audit Manager [framework sharing concepts and terminology](#).
- The custom framework that you want to share is [eligible for sharing](#) and exists in the framework library of your AWS Audit Manager environment.
- The recipient already enabled AWS Audit Manager in the AWS Region where you want to share the custom framework.
- The recipient is not an AWS Organizations management account.

Tip

Before you start, make a note of the AWS account ID that you want to share your custom framework with. This can be your own account ID, if your goal is to replicate the framework to another AWS Region under your account. You need this information for step 2 of the tutorial.

Important

Don't share custom frameworks that contain sensitive data. This includes data found within the framework itself, its control sets, and any of the custom controls that comprise the custom framework. For more information, see [Framework eligibility](#).

Step 1: Identify the custom framework that you want to share

Start by identifying the custom framework that you want to share. You can find a list of all available custom frameworks on the **Framework library** page in Audit Manager.

To view your available custom frameworks

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Framework library**.
3. Choose the **Custom frameworks** tab. This displays a list of your available custom frameworks. You can choose any framework name to view the details of that custom framework.

Step 2: Send a share request

Next, specify a recipient and send them a share request for the custom framework. The recipient has 120 days to respond to the share request before it expires.

To send a share request

1. From the **Custom frameworks** tab of the framework library, choose the name of a framework to open the detail page. From here, choose **Actions** and then choose **Share custom framework**.
 - Alternatively, select a custom framework from the list in the framework library, choose **Actions**, and then choose **Share custom framework**. Depending on the size of the custom framework, this method can take a few seconds while Audit Manager prepares the share request.
2. Review the notice that displays in the dialog box.
 - If you're unsure whether you can share your custom framework, review [Framework eligibility](#) for further guidance.
 - If your framework has controls that use custom AWS Config rules as a data source, we recommend that you contact the recipient to let them know. The recipient can then create and enable the same AWS Config rules in their instance of AWS Config. For more information, see [My shared framework has controls that use custom AWS Config rules as a data source. Can the recipient collect evidence for these controls? \(p. 302\)](#).

3. Enter **agree** and then choose **Agree** to proceed.
4. On the next screen, follow these steps:
 - Under **AWS account**, enter the recipient's account ID. This can be your own account ID.
 - Under **AWS Region**, select the recipient's Region from the dropdown list.
 - (Optional) Under **Message to recipient**, enter an optional comment about the custom framework that you're sharing.
 - Under **Custom framework details**, review the details to confirm that you want to share this framework.
5. Choose **Share**.

Note

Keep in mind the following points:

- When you share a custom framework with another AWS account, the framework is replicated only to the specified AWS Region. After accepting the share request, the recipient can then replicate the framework across Regions as needed.
- When sharing custom frameworks across AWS Regions, it can take up to 10 minutes to process share request actions. After sending a cross-Region share request, we recommend that you check back later to confirm that your share request was sent successfully.
- When you send a share request, Audit Manager takes a snapshot of the custom framework at the time of the share request creation. If you update the custom framework after sending a share request, the request isn't automatically updated. To share the latest version of an updated framework, you can [resend the share request](#). The expiration date of this new snapshot is 120 days from the re-share date.

Step 3: View your sent requests

You can select the **Sent requests** tab to see a list of all the share requests that you sent. You can filter this list as needed. For example, you can apply filters to display only requests that expire within the next 30 days.

To view and filter your sent requests

1. From the navigation pane, choose **Share requests**.
2. Choose the **Sent requests** tab.
3. (Optional) Apply filters to fine-tune which sent requests are visible. You can do this by finding the **All statuses** dropdown list, and changing the filter to one of the following.
 - **Active** – This filter displays share requests that are awaiting a response from the recipient.
 - **Shared** – This filter displays share requests that were accepted by the recipient. The shared custom framework now exists in the recipient's framework library.
 - **Inactive** – This filter displays share requests that were declined, revoked, or expired before the recipient took action. Choose the word **Inactive** to view more details.
 - **Expiring** – This filter displays share requests that expire in the next 30 days.
 - **Failed** – This filter displays the share requests that weren't successfully sent to the recipient. Choose the word **Failed** to view more details.

Note

It can take up to 15 minutes to process a share request. As a result, if an error occurred when sending your share request to the recipient, the *Failed* status might not display immediately. We recommend that you check back later to confirm that your share request was sent successfully.

For information about how to proceed if you encounter an error, see [Troubleshooting share requests](#).

Step 4 (Optional): Revoke the share request

If you need to cancel an active share request before it's due to expire, you can revoke the request at any time. This step is optional. If you take no action, the recipient loses the ability to accept the share request after the expiration date.

To revoke a share request

1. From the navigation pane, choose **Share requests**.
2. Choose the **Sent requests** tab.
3. Select the framework that you want to revoke and choose **Revoke request**.
4. In the pop-up window that appears, choose **Revoke**.

Note

You can only revoke access to share requests that have a status of *Active* or *Expiring*. After a recipient accepts a share request, you can no longer revoke their access to that custom framework. This is because a copy of the custom framework now exists in the recipient's framework library.

When sharing frameworks across AWS Regions, it can take up to 10 minutes to process share request actions. After revoking a cross-Region share request, we recommend that you check back later to confirm that the share request was revoked successfully.

Resending a share request for an updated framework

You might send a share request for a custom framework and then update the same framework afterwards. If you do this, the share request isn't automatically updated to reflect the latest version of the framework. However, if its status is *active*, *shared*, or *expiring*, you can update an existing share request. To do this, you resend a new share request with the same set of details as the existing request. In the new share request, include the same custom framework ID, recipient account ID, and recipient AWS Region. You can also provide a new comment with the new share request.

Keep in mind the following when you resend a share request:

- For the update to be successful, the new request must be for the same custom framework ID. It must also specify the same recipient account ID and Region as the existing request.
- If the name of the custom framework has changed, the updated share request displays the latest name.
- If you provide a new comment, the updated share request displays the latest comment.
- When you resend a share request, the expiration date is extended by six months.

To resend a share request for an updated framework

1. From the **Custom frameworks** tab of the framework library, choose the name of the framework that you want to share. This opens the framework detail page. From here, choose **Actions** and then choose **Share custom framework**.
 - Alternatively, select the custom framework from the list in the framework library, choose **Actions**, and then choose **Share custom framework**. Depending on the size of the custom framework, this method can take a few seconds for Audit Manager to prepare the share request.
2. Review the notice that displays in the dialog box, enter **agree**, and then choose **Agree** to proceed.
3. On the next screen, follow these steps:

- Under **AWS account**, enter the same account ID that you specified in the existing share request.
 - Under **AWS Region**, select the same Region that you specified in the existing share request.
 - (Optional) Under **Message to recipient**, enter an optional comment about the updated custom framework.
 - Under **Custom framework details**, review the details to confirm that you want to resend the share request.
4. Choose **Share** to resend and update the share request.

Troubleshooting share requests

To find solutions to the issues that you might encounter when sharing a custom framework, see [Troubleshooting framework sharing issues \(p. 300\)](#) in the *Troubleshooting* section of this guide.

Responding to share requests

This tutorial describes the actions to take when you receive a share request for a custom framework. Audit Manager notifies you when you receive a share request. You also receive a notification to remind you when a share request is due to expire in the next 30 days.

This tutorial covers the following steps:

1. [Check your share request notifications](#) – Review a list of share requests that are active and expiring soon.
2. [Take action on the share request](#) – Accept or decline the share request for the custom framework.
3. [View the share requests that you've received from others](#) – View your share request history.

Prerequisites

Before you get started, we recommend that you first learn more about Audit Manager [framework sharing concepts and terminology](#).

Step 1: Check your received request notifications

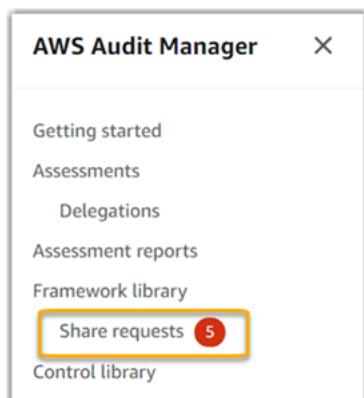
Start by checking your share request notifications. The **Received requests** tab displays a list of the share requests that you've received from other AWS accounts. Requests that are awaiting your response appear with a blue dot. You can also filter this view to display only requests that expire sometime within the next 30 days.

To view received requests

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. If you have a share request notification, Audit Manager displays a red dot next to the navigation menu icon.



3. Expand the navigation pane and look next to **Share requests**. A notification badge indicates the number of share requests that need your attention.



4. Choose **Share requests**. By default, this page opens on the **Received requests** tab.
5. Identify the share requests that need your action by looking for items with a blue dot.

Received requests (21) Info			
	Framework name	Request status	Expiration date
<input type="radio"/>	FrameworkShare-CustomStandardMix	● Active	January 11, 2022, 8:37 AM UTC
<input type="radio"/>	FrameworkShare-CustomStandardMix	● Active	January 11, 2022, 8:35 AM UTC

6. (Optional) To view only requests that expire in the next 30 days, find the **All statuses** dropdown list and select **Expiring**.

Step 2: Take action on the request

To remove the blue notification dot, you need to take action by either accepting or declining the share request.

Note

It can take up to 10 minutes to process share request actions when a framework is shared across AWS Regions. After taking action on a cross-Region share request, we recommend that you check back later to confirm that the share request was successfully accepted or declined.

Accepting a shared framework

When you accept a share request, Audit Manager replicates a snapshot of the original framework into the custom frameworks tab of your framework library. Audit Manager replicates and encrypts the new custom framework using the KMS key that you specified in your [Audit Manager settings](#).

To accept a share request

1. Open the **Share requests** page and make sure that you're viewing the **Received requests** tab.
2. (Optional) Select **Active** or **Expiring** from the filter dropdown list.
3. (Optional) Choose a framework name to view the details of the share request. This includes information such as the framework description, the number of controls that are in the framework, and the message from the sender.
4. Select the share request that you want to accept, choose **Actions**, and then choose **Accept**.

After you accept a share request, the status changes to *replicating* while the shared custom framework is added to your framework library. If the framework contains custom controls, these controls are added to your control library at this time.

When the framework replication is complete, the status changes to *shared*. A success banner notifies you that the custom framework is ready to use.

Tip

When you accept a custom framework, it's replicated only to your current AWS Region. You might want the new shared framework to be available across all Regions in your AWS account. If so, after you accept the share request you can [share the framework](#) to other Regions under your account as needed.

Declining a shared framework

When you decline a share request, Audit Manager doesn't add that custom framework to your framework library. However, a record of the declined share request remains in the **Received requests** tab, with a status of **Inactive**.

To decline a share request

1. Open the **Share requests** page and make sure that you're viewing the **Received requests** tab.
2. (Optional) Select **Active** or **Expiring** from the filter dropdown list.
3. (Optional) Choose a framework name to view the details of the share request. This includes information such as the framework description, the number of controls that are in the framework, and the message from the sender.
4. Select the share request that you want to decline, choose **Actions**, and then choose **Decline**.
5. In the dialog box that appears, choose **Decline** to confirm your choice.

Tip

If you change your mind and want access to a shared framework after you decline, ask the sender to send you a new share request.

Step 3: View a history of your received requests

After you accept or decline a shared framework, you can return to the **Share requests** page to see your share request history. You can filter this list as needed. For example, you can apply filters to display only requests that you accepted.

To view a history of your share requests

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the left navigation pane, choose **Share requests**.
3. Choose the **Received requests** tab.
4. Find the **All statuses** dropdown list, and select one of the following filters.
 - **Active** – This filter displays share requests that you haven't yet accepted or declined.
 - **Expiring** – This filter displays share requests that expire in the next 30 days.
 - **Shared** – This filter displays share requests that you accepted. The shared framework is now available in your framework library.
 - **Inactive** – This filter displays share requests that were declined or expired.
 - **Failed** – This filter displays the share requests that weren't sent successfully. Choose the word **Failed** to view more details.

What can I do next?

After you accept a shared custom framework, you can find it in the custom frameworks tab of the framework library. You can now use that framework to create an assessment. To learn more, see [Creating an assessment](#). For instructions on how to edit your new custom framework, see [Editing a custom framework](#).

Deleting share requests

You can delete share requests that are no longer wanted or needed.

Note

You can't delete share requests that have a status of *active* or *replicating*.

When you delete a share request, only the request itself is deleted. The shared framework itself remains in your framework library.

To delete a share request

1. From the navigation pane, choose **Share requests**.
2. Choose either the **Sent requests** or the **Received requests** tab.
3. Select the framework that you no longer want and choose **Delete**.
4. In the pop-up window that appears, choose **Delete**.

Supported frameworks in AWS Audit Manager

AWS Audit Manager provides the following standard frameworks. These prebuilt frameworks are based on AWS best practices for various compliance standards and regulations. You can use these frameworks to assist you with your audit preparation.

Topics

- [Australian Cyber Security Centre \(ACSC\) Essential Eight \(p. 128\)](#)
- [Australian Cyber Security Centre \(ACSC\) Information Security Manual \(p. 129\)](#)
- [AWS Audit Manager Sample Framework \(p. 131\)](#)
- [AWS Control Tower Guardrails \(p. 132\)](#)
- [AWS generative AI best practices framework v1 \(p. 133\)](#)
- [AWS License Manager \(p. 138\)](#)
- [AWS Foundational Security Best Practices \(p. 140\)](#)
- [AWS Operational Best Practices \(p. 141\)](#)
- [AWS Well-Architected \(p. 142\)](#)
- [Canadian Centre for Cyber Security Medium Cloud Control Profile \(p. 144\)](#)
- [CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.2.0 \(p. 145\)](#)
- [CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0 \(p. 151\)](#)
- [CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4.0 \(p. 154\)](#)
- [CIS Controls v7.1 Implementation Group 1 \(p. 156\)](#)
- [CIS Controls v8 Implementation Group 1 \(p. 158\)](#)
- [FedRAMP Moderate Baseline \(p. 160\)](#)
- [General Data Protection Regulation \(GDPR\) \(p. 162\)](#)
- [Gramm-Leach-Bliley Act \(p. 180\)](#)
- [GxP 21 CFR part 11 \(p. 181\)](#)

- [GxP EU Annex 11 \(p. 183\)](#)
- [Health Insurance Portability and Accountability Act \(HIPAA\) Security Rule 2003 \(p. 185\)](#)
- [Health Insurance Portability and Accountability Act \(HIPAA\) Final Omnibus Security Rule 2013 \(p. 187\)](#)
- [ISO/IEC 27001:2013 Annex A \(p. 189\)](#)
- [NIST 800-53 \(Rev. 5\) Low-Moderate-High \(p. 190\)](#)
- [NIST Cybersecurity Framework version 1.1 \(p. 192\)](#)
- [NIST SP 800-171 \(Rev. 2\) \(p. 194\)](#)
- [PCI DSS V3.2.1 \(p. 196\)](#)
- [SOC 2 \(p. 197\)](#)

Australian Cyber Security Centre (ACSC) Essential Eight

To assist you with your audit preparation, AWS Audit Manager provides a prebuilt standard framework that structures and automates assessments for the Essential Eight framework.

Topics

- [What is the Australian Cyber Security Centre \(ACSC\) Essential Eight? \(p. 128\)](#)
- [Using this framework to support your audit preparation \(p. 128\)](#)
- [More Essential Eight resources \(p. 129\)](#)

What is the Australian Cyber Security Centre (ACSC) Essential Eight?

The Australian Cyber Security Centre (ACSC) is the Australian government's lead agency for cyber security. To protect against cyber threats, the ACSC recommends that organizations implement eight essential mitigation strategies from the ACSC's *Strategies to Mitigate Cyber Security Incidents* as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise systems.

As the Essential Eight outlines a minimum set of preventative measures, your organization needs to implement additional measures where it is warranted by your environment. Further, while the Essential Eight can help to mitigate the majority of cyber threats, it will not mitigate all cyber threats. As such, additional mitigation strategies and security controls need to be considered, including those from the *Strategies to Mitigate Cyber Security Incidents* and the *Information Security Manual* (ISM).

The [Essential Eight](#) by the [ACSC](#) is licensed under a [Creative Commons Attribution 4.0 International License](#) and copyright information can be found at [ACSC | Copyright](#). © Commonwealth of Australia 2022.

Using this framework to support your audit preparation

You can use the Essential Eight standard framework in AWS Audit Manager to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to Essential Eight requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts

to assess your AWS resources. It does this based on the controls that are defined in the Essential Eight framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
Essential Eight	7	1	8	<ul style="list-style-type: none">• AWS Config• AWS Security Hub

Tip

To review the AWS Config rules that are used as data source mappings in this standard framework, download the [AuditManager_ConfigDataSourceMappings_EssentialEight.zip](#) file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with the Essential Eight controls. Moreover, they can't guarantee that you'll pass an Essential Eight audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find the Essential Eight framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the Essential Eight framework. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#). For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More Essential Eight resources

- [ACSC Essential Eight](#)

Australian Cyber Security Centre (ACSC) Information Security Manual

To assist you with your audit preparation, AWS Audit Manager provides a prebuilt standard framework that structures and automates assessments for the ACSC Information Security Manual framework.

Topics

- [What is the Australian Cyber Security Centre \(ACSC\) Information Security Manual? \(p. 130\)](#)
- [Using this framework to support your audit preparation \(p. 130\)](#)

- [More ACSC Information Security Manual resources \(p. 131\)](#)

What is the Australian Cyber Security Centre (ACSC) Information Security Manual?

The Australian Cyber Security Centre (ACSC) is the Australian government's lead agency for cyber security. The ACSC produces the Information Security Manual (ISM), which functions as a set of cyber security principles. The purpose of these principles is to provide strategic guidance on how an organization can protect their systems and data from cyber threats. These cyber security principles are grouped into four key activities: govern, protect, detect and respond. An organization should be able to demonstrate that the cyber security principles are being adhered to within their organization. The ISM is intended for Chief Information Security Officers, Chief Information Officers, cyber security professionals, and information technology managers.

The ISM framework is provided by the Australian Cyber Security Centre under a [Creative Commons Attribution 4.0 International License](#), and copyright information can be found at [ACSC | Copyright](#). © Commonwealth of Australia 2022.

Using this framework to support your audit preparation

You can use the ACSC Information Security Manual standard framework in AWS Audit Manager to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to ACSC Information Security Manual requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the ACSC Information Security Manual framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
ACSC Information Security Manual	45	396	22	<ul style="list-style-type: none">• Amazon Elastic Compute Cloud• AWS Config• AWS Identity and Access Management

Tip

To review the AWS Config rules that are used as data source mappings in this standard framework, download the [AuditManager_ConfigDataSourceMappings_ACSC-Information-Security-Manual.zip](#) file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with the ACSC Information Security Manual controls. Moreover, they can't guarantee that you'll pass an ACSC audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find the ACSC Information Security Manual framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the ACSC Information Security Manual framework. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#). For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More ACSC Information Security Manual resources

- [ACSC Information Security Manual](#)

AWS Audit Manager Sample Framework

AWS Audit Manager provides a sample framework to help you get started with your audit preparation.

Topics

- [What is the AWS Audit Manager Sample Framework? \(p. 131\)](#)
- [Using this framework to support your audit preparation \(p. 131\)](#)

What is the AWS Audit Manager Sample Framework?

The *AWS Audit Manager Sample Framework* is a simple framework that you can use to get started in Audit Manager. Some of the other prebuilt frameworks that Audit Manager provides, in comparison, are much larger and contain numerous controls. By using the sample framework instead of these larger frameworks, you can more easily review and explore an example of a framework. The controls in this framework are based around a series of AWS Config and AWS API calls.

Using this framework to support your audit preparation

You can use this framework to help you get started in AWS Audit Manager. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the *AWS Audit Manager Sample Framework* as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the framework. Next, it collects the relevant evidence and then attaches it to the controls in your assessment.

The AWS Audit Manager Sample Framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
AWS Audit Manager Sample Framework	4	1	3	<ul style="list-style-type: none">• Amazon Elastic Compute Cloud

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
				<ul style="list-style-type: none">AWS CloudTrailAWS Identity and Access Management

You can find this framework under the [Standard frameworks tab of the Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the AWS Audit Manager Sample Framework. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

AWS Control Tower Guardrails

AWS Audit Manager provides an AWS Control Tower Guardrails framework to assist you with your audit preparation.

Topics

- [What is AWS Control Tower? \(p. 132\)](#)
- [Using this framework to support your audit preparation \(p. 132\)](#)
- [More AWS Control Tower resources \(p. 133\)](#)

What is AWS Control Tower?

AWS Control Tower is a management and governance service that you can use to navigate through the setup process and governance requirements that are involved in creating a multi-account AWS environment.

With AWS Control Tower, you can provision new AWS accounts that conform to your company- or organization-wide policies in a few clicks. AWS Control Tower creates an *orchestration* layer on your behalf that combines and integrates the capabilities of several other [AWS services](#). These services include AWS Organizations, AWS IAM Identity Center, and AWS service Catalog. This helps streamline the process of setting up and governing a multi-account AWS environment that's both secure and compliant.

The AWS Control Tower Guardrails framework contains all of the AWS Config Rules that are based on guardrails from AWS Control Tower.

Using this framework to support your audit preparation

You can use the *AWS Control Tower Guardrails* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are

grouped according to the AWS Config Rules that are based on guardrails from AWS Control Tower. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for an AWS Control Tower audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the AWS Control Tower Guardrails framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The AWS Control Tower Guardrails framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
AWS Control Tower Guardrails	14	0	5	AWS Config

Tip

To review the AWS Config rules that are used as data source mappings in this standard framework, download the [AuditManager_ConfigDataSourceMappings_ControlTowerGuardrails.zip](#) file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with AWS Control Tower Guardrails. Moreover, they can't guarantee that you'll pass an audit.

You can find the AWS Control Tower Guardrails framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create or update an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the AWS Control Tower Guardrails. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More AWS Control Tower resources

- [AWS Control Tower service page](#)
- [AWS Control Tower user guide](#)

AWS generative AI best practices framework v1

AWS Audit Manager provides a prebuilt standard framework to help you gain visibility into how your generative AI implementation on Amazon Bedrock is working against AWS recommended best practices.

Amazon Bedrock is a fully managed service that makes AI models from Amazon and other leading AI companies available through an API. With Amazon Bedrock, you can privately tune existing models

with your organization's data. This enables you to harness foundation models (FMs) and large language models (LLMs) to build applications securely, without compromising data privacy. For more information, see [What is Amazon Bedrock?](#) in the *Amazon Bedrock User Guide*.

Topics

- [What are AWS generative AI best practices for Amazon Bedrock? \(p. 134\)](#)
- [Using this framework to support your audit preparation \(p. 135\)](#)
- [Manually verifying prompts in Amazon Bedrock \(p. 136\)](#)
- [More resources \(p. 138\)](#)

What are AWS generative AI best practices for Amazon Bedrock?

Generative AI refers to a branch of AI that focuses on enabling machines to generate content. Generative AI models are designed to create outputs that closely resemble the examples that they were trained on. This creates scenarios where AI can mimic human conversation, generate creative content, analyze vast volumes of data, and automate processes that are normally done by humans. The rapid growth of generative AI brings promising new innovation. At the same time, it raises new challenges around how to use generative AI responsibly and in compliance with governance requirements.

AWS is committed to providing you with the tools and guidance needed to build and govern applications responsibly. To help you with this goal, Audit Manager has partnered with Amazon Bedrock to create the **AWS generative AI best practices framework v1**. This framework provides you with a purpose-built tool for monitoring and improving the governance of your generative AI projects on Amazon Bedrock. You can use the best practices in this framework to gain tighter control and visibility over your model usage and stay informed on model behavior.

The controls in this framework were developed in collaboration with AI experts, compliance practitioners, security assurance specialists across AWS, and with input from Deloitte. Each automated control maps to an AWS data source from which Audit Manager collects evidence. You can use the collected evidence to evaluate your generative AI implementation based on the following eight principles:

1. **Responsible** – Develop and adhere to ethical guidelines for the deployment and usage of generative AI models
2. **Safe** – Establish clear parameters and ethical boundaries to prevent the generation of harmful or problematic output
3. **Fair** – Consider and respect how an AI system impacts different sub-populations of users
4. **Sustainable** – Strive for greater efficiency and more sustainable power sources
5. **Resilience** – Maintain integrity and availability mechanisms to ensure an AI system operates reliably
6. **Privacy** – Ensure that sensitive data is protected from theft and exposure
7. **Accuracy** – Build AI systems that are accurate, reliable, and robust
8. **Secure** – Prevent unauthorized access to generative AI systems

Example

Let's say that your application uses a third-party foundational model that's available on Amazon Bedrock. You can use the AWS generative AI best practices framework to monitor your usage of this model. By using this framework, you can collect evidence that demonstrates that your usage is compliant with generative AI best practices. This provides you with a consistent approach for tracking model usage and permissions, flagging sensitive data, and being alerted about any inadvertent disclosures. For instance, specific controls in this framework can collect evidence that helps you show that you've implemented mechanisms for the following:

- Documenting the source, nature, quality, and treatment of the new data, to ensure transparency and help in troubleshooting or audits (*Responsible*)

- Regularly evaluating the model using predefined performance metrics to ensure it meets accuracy and safety benchmarks (*Safe*)
- Using automated monitoring tools to detect and alert on potential biased outcomes or behaviors in real-time (*Fair*)
- Evaluating, identifying, and documenting model usage and scenarios where existing models can be reused, whether you generated them or not (*Sustainable*)
- Setting up procedures for notification if there is inadvertent PII spillage or unintentional disclosure (*Privacy*)
- Establishing real-time monitoring of the AI system and setting up alerts for any anomalies or disruptions (*Resilience*)
- Detecting inaccuracies, and conducting a thorough error analysis to understand the root causes (*Accuracy*)
- Implementing end-to-end encryption for input and output data of the AI models to minimum industry standards (*Secure*)

Using this framework to support your audit preparation

Note

- If you're an Amazon Bedrock customer, you can use this framework directly in Audit Manager. Make sure that you use the framework and run assessments in the AWS accounts and Regions where you run your generative AI models and applications.
- If you want to encrypt your CloudWatch logs for Amazon Bedrock with your own KMS key, make sure that Audit Manager has access to that key. To do this, you can save your customer managed key in your Audit Manager [Data encryption \(p. 252\)](#) settings.
- This framework uses the Amazon Bedrock [ListCustomModels](#) operation to generate evidence about your custom model usage. This API operation is currently supported in the US East (N. Virginia) and US West (Oregon) AWS Regions only. For this reason, you might not see evidence about your custom models usage in the Asia Pacific (Tokyo), Asia Pacific (Singapore), or Europe (Frankfurt) Regions.

You can use this framework to help you prepare for audits about your usage of generative AI on Amazon Bedrock. It includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to generative AI best practices. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that helps you monitor compliance with your intended policies. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the AWS generative AI Best Practices framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of control sets	Number of automated controls	Number of manual controls
AWS Generative AI Best Practices Framework v1	8	34 fully automated 18 partially automated	58

Tip

To learn more about automated and manual controls, see [Audit Manager concepts and terminology](#) for an example of when it's recommended to add manual evidence to a partially automated control.

To review the AWS Config rules that are used as control data source mappings in this standard framework, download the [AuditManager_ConfigDataSourceMappings_AWS-Generative-AI-Best-Practices.zip](#) file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with generative AI best practices. Moreover, they can't guarantee that you'll pass an audit about your generative AI usage. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find this framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#). For instructions on how to make an editable copy of this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

Manually verifying prompts in Amazon Bedrock

You might have different sets of prompts that you need to evaluate against specific models. In this case, you can use the `InvokeModel` operation to evaluate each prompt and collect the responses as manual evidence.

Using the `InvokeModel` operation

To get started, create a list of predefined prompts. You'll use these prompts to verify the model's responses. Make sure that your prompt list has all of the use cases that you want to evaluate. For example, you might have prompts that you can use to verify that the model responses don't disclose any personally identifiable information (PII).

After you create your list of prompts, test each one using the `InvokeModel` operation that Amazon Bedrock provides. You can then collect the model's responses to these prompts, and [upload this data as manual evidence](#) in your Audit Manager assessment.

There are three different ways to use the `InvokeModel` operation.

1. HTTP Request

You can use tools like Postman to create a HTTP request call to `InvokeModel` and store the response.

Note

Postman is developed by a third-party company. It isn't developed or supported by AWS. To learn more about using Postman, or for assistance with issues related to Postman, see the [Support center](#) on the Postman website.

2. AWS CLI

You can use the AWS CLI to run the `invoke-model` command. For instructions and more information, see [Running inference on a model](#) in the *Amazon Bedrock User Guide*.

The following example shows how to generate text with the AWS CLI using the prompt "*story of two dogs*" and the *Anthropic Claude V2* model. The example returns up to *300* tokens in the response and saves the response to the 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:\",\n\"max_tokens_to_sample\" : 300}\"\n--cli-binary-format raw-in-base64-out\ninvoke-model-output.txt
```

3. Automated verification

You can use CloudWatch Synthetics canaries to monitor your model responses. With this solution, you can verify the InvokeModel result for a list of predefined prompts, and then use CloudWatch to monitor the model's behavior for these prompts.

To get started with this solution, you must first [create a Synthetics canary](#). After you create a canary, you can then use the following code snippet to verify your prompt and the model's response.

```
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

Alternatively, you can also use a Lambda function to run this script. If you choose this solution, you'll need to [create a Lambda function](#) first.

Sample prompts

You can use these sample prompts as a starting point to test your model's responses. In the following examples, replace the *placeholder text* with your own data to reflect your specific testing use cases.

To test for inappropriate content in model responses

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

To test for PII in model responses

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

To test for profanity in model responses

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

More resources

- [Amazon Bedrock](#)
- [Amazon Bedrock User Guide](#)
- [Transform responsible AI from theory into practice](#)
- [Protecting Consumers and Promoting Innovation – AI Regulation and Building Trust in Responsible AI](#)
- [Responsible Use of Machine Learning guide](#)

AWS License Manager

AWS Audit Manager provides an AWS License Manager framework to assist you with your audit preparation.

Topics

- [What is AWS License Manager? \(p. 138\)](#)
- [Using this framework to support your audit preparation \(p. 138\)](#)
- [More AWS License Manager resources \(p. 139\)](#)

What is AWS License Manager?

With AWS License Manager, you can manage your software licenses from various software vendors (such as Microsoft, SAP, Oracle, or IBM) centrally across AWS and on-premises environments. Having all your software licenses in one location allows for better control and visibility and potentially helps you to limit licensing overages and reduce the risk of non-compliance and misreporting issues.

The AWS License Manager framework is integrated with License Manager to aggregate license usage information based on customer defined licensing rules.

Using this framework to support your audit preparation

You can use the *AWS License Manager* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped according to customer defined licensing rules. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the AWS License Manager framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The AWS License Manager framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
AWS License Manager	27	0	6	AWS License Manager

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with licensing rules. Moreover, they can't guarantee that you'll pass a licensing usage audit.

You can find this framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the AWS License Manager framework. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More AWS License Manager resources

License Manager links

- [AWS License Manager service page](#)
- [AWS License Manager user guide](#)

License Manager APIs

For this framework, Audit Manager uses a custom activity called `GetLicenseManagerSummary` to collect evidence. The `GetLicenseManagerSummary` activity calls the following three License Manager APIs:

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

The data that's returned is then converted into evidence and attached to the relevant controls in your assessment.

For example: Let's say that you use two licensed products (*SQL Server 2017* and *Oracle Database Enterprise Edition*). First, the `GetLicenseManagerSummary` activity calls the [ListLicenseConfigurations](#) API, which provides details of license configurations in your account. Next, it adds additional contextual data for each license configuration by calling [ListUsageForLicenseConfiguration](#) and [ListAssociationsForLicenseConfiguration](#). Finally, it converts the license configuration data into evidence and attaches it to the respective controls in the framework (4.5 - *Customer managed license for SQL Server 2017* and 3.0.4 - *Customer managed license for Oracle Database Enterprise Edition*). If you're using

a licensed product that isn't covered by any of the controls in the framework, that license configuration data is attached as evidence to the following control: *5.0 - Customer managed license for other licenses*.

AWS Foundational Security Best Practices

AWS Audit Manager provides a prebuilt standard framework that supports the AWS Foundational Security Best Practices.

Topics

- [What is the AWS Foundational Security Best Practices standard? \(p. 140\)](#)
- [Using this framework to support your audit preparation \(p. 140\)](#)
- [More AWS Foundational Security Best Practices resources \(p. 141\)](#)

What is the AWS Foundational Security Best Practices standard?

The AWS Foundational Security Best Practices standard is a set of controls that detect when your deployed accounts and resources deviate from security best practices.

You can use this standard to continually evaluate all of your AWS accounts and workloads and quickly identify areas of deviation from best practices. The standard provides actionable and prescriptive guidance on how to improve and maintain your organization's security posture.

The controls include best practices from across multiple AWS services. Each control is assigned a category that reflects the security function that it applies to. For more information, see [Control categories](#) in the *AWS Security Hub User Guide*.

Using this framework to support your audit preparation

You can use the *AWS Foundational Security Best Practices* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to AWS Foundational Security Best Practices requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess resources in your AWS accounts and services. It does this based on the controls that are defined in the AWS Foundational Security Best Practices framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The AWS Foundational Security Best Practices framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
AWS Foundational Security Best Practices	154	0	29	AWS Security Hub

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with AWS Foundational Security Best Practices. Moreover, they can't guarantee that you'll pass an AWS Foundational Security Best Practices audit.

You can find this framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the AWS Foundational Security Best Practices. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More AWS Foundational Security Best Practices resources

- [AWS Foundational Security Best Practices standard](#) in the *AWS Security Hub User Guide*
- [Control categories](#) in the *AWS Security Hub User Guide*

AWS Operational Best Practices

AWS Audit Manager provides a prebuilt AWS Operational Best Practices (OBP) framework to assist you with your audit preparation. This framework offers a subset of controls from the AWS Foundational Security Best Practices standard. These controls serve as baseline checks to detect when your deployed accounts and resources deviate from security best practices.

Topics

- [What is the AWS Foundational Security Best Practices standard? \(p. 141\)](#)
- [Using this framework to support your audit preparation \(p. 141\)](#)
- [More AWS OBP resources \(p. 142\)](#)

What is the AWS Foundational Security Best Practices standard?

You can use the *AWS Foundational Security Best Practices* standard to evaluate your accounts and workloads and quickly identify areas of deviation from best practices. The standard provides actionable and prescriptive guidance on how to improve and maintain your organization's security posture.

The controls include best practices from across multiple AWS services. Each control is assigned a category that reflects the security function that it applies to. For more information, see [Control categories](#) in the *AWS Security Hub User Guide*.

Using this framework to support your audit preparation

You can use the *AWS Operational Best Practices* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to AWS Operational Best Practices requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess resources in your AWS accounts and services. It does this based on the controls that are defined in the AWS Operational Best Practices framework. When it's time for an audit, you—or a delegate of

your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The AWS Operational Best Practices framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
AWS Operational Best Practices	52	0	20	AWS Security Hub

The controls in this framework aren't intended to verify if your systems are compliant with AWS Operational Best Practices. Moreover, they can't guarantee that you'll pass an AWS Operational Best Practices audit.

You can find this framework under the [Standard frameworks tab of the Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the AWS Operational Best Practices. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More AWS OBP resources

- [AWS Foundational Security Best Practices standard](#) in the [AWS Security Hub User Guide](#)
- [Control categories](#) in the [AWS Security Hub User Guide](#)

AWS Well-Architected

AWS Audit Manager provides a prebuilt framework that structures and automates assessments for the AWS Well-Architected Framework, based on AWS best practices.

Topics

- [What is AWS Well-Architected? \(p. 142\)](#)
- [Using this framework to support your audit preparation \(p. 143\)](#)
- [More AWS Well-Architected resources \(p. 141\)](#)

What is AWS Well-Architected?

[AWS Well-Architected](#) is a framework that can help you to build secure, high-performing, resilient, and efficient infrastructure for your applications and workloads. Based on six pillars—operational excellence,

security, reliability, performance efficiency, cost optimization, and sustainability—AWS Well-Architected provides a consistent approach for you and your partners to evaluate architectures and implement designs that can scale over time.

Using this framework to support your audit preparation

You can use the *AWS Well-Architected Framework* to help you prepare for audits. This framework describes the key concepts, design principles, and architectural best practices for designing and running workloads in the cloud. Out of the six pillars that AWS Well-Architected is based on, the security and reliability pillars are the pillars that AWS Audit Manager offers a prebuilt framework and controls for. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the AWS Well-Architected Framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The AWS Well-Architected Framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
AWS Well-Architected Framework	16	0	2	AWS Config

Tip

To review the AWS Config rules that are used as data source mappings in this standard framework, download the [AuditManager_ConfigDataSourceMappings_AWSWell-ArchitectedFramework.zip](#) file.

The controls in this framework aren't intended to verify if your systems are compliant. Moreover, they can't guarantee that you'll pass an audit that's associated with the AWS Well-Architected Framework.

You can find this framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the AWS Well-Architected Framework. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More AWS Well-Architected resources

- [AWS Well-Architected](#)
- [AWS Well-Architected Framework documentation](#)

Canadian Centre for Cyber Security Medium Cloud Control Profile

AWS Audit Manager provides a prebuilt standard framework that structures and automates assessments for the Canadian Centre for Cyber Security.

Topics

- [What is the Canadian Centre for Cyber Security? \(p. 144\)](#)
- [Using this framework to support your audit preparation \(p. 144\)](#)

What is the Canadian Centre for Cyber Security?

The Canadian Centre for Cyber Security (CCCS) is Canada's authoritative source of cybersecurity expert guidance, services, and support. CCCS provides this expertise to Canadian governments, industry, and the general public. Their rigorous assessments of cloud service providers are relied on by Canadian public sector organizations across the country to make informed cloud procurement decisions.

The CCCS Medium Cloud Control Profile replaced the government of Canada's PROTECTED B / Medium Integrity / Medium Availability (PBMM) profile in May 2020. The CCCS Medium Cloud Security Control Profile is suitable if your organization uses public cloud services to support business activities with medium confidentiality, integrity, and availability (AIC) requirements. Workloads with medium AIC requirements mean that unauthorized disclosure, modification, or loss of access to the information or services that are used by the business activity can reasonably be expected to cause serious injury to an individual or organization or limited injury to a group of individuals. Examples of these levels of injury include the following:

- Significant effect on annual profit
- Loss of major accounts
- Loss of goodwill
- Clear compliance violation
- Privacy violation for hundreds or thousands of people
- Affects program performance
- Causing mental disorder or illness
- Sabotage
- Damage to reputation
- Individual financial hardship

Using this framework to support your audit preparation

You can use the AWS Audit Manager framework for the Medium Cloud Control Profile to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to CCCS requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for a CCCS Medium Cloud Control Profile audit. In your assessment, you can specify the AWS accounts and services that you want to include in the scope of your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the CCCS Medium Cloud Control Profile framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
Canadian Centre for Cyber Security - Medium	206	396	165	<ul style="list-style-type: none"> • Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Key Management Service • AWS License Manager

Tip

To review the AWS Config rules that are used as data source mappings in this standard framework, download the [AuditManager_ConfigDataSourceMappings_CanadianCentreforCyberSecurity-Medium.zip](#) file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with the CCCS Medium Cloud Control Profile standard. Moreover, they can't guarantee that you'll pass an CCCS audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find this framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the Canadian Centre for Cyber Security - Medium framework. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.2.0

AWS Audit Manager provides two prebuilt frameworks that support the CIS AWS Foundations Benchmark v1.2.0:

- *CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.2.0, Level 1*

- CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.2.0, Level 1 and 2

Note

- For information about the Audit Manager frameworks that support v1.3.0, see [CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0 \(p. 151\)](#).
- For information about the Audit Manager frameworks that support v1.4.0, see [CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4.0 \(p. 154\)](#).

Topics

- [What is CIS? \(p. 146\)](#)
- [Using these frameworks to support your audit preparation \(p. 146\)](#)
- [More CIS resources \(p. 151\)](#)

What is CIS?

The *Center for Internet Security (CIS)* is a nonprofit that developed the [CIS AWS Foundations Benchmark](#). This benchmark serves as a set of security configuration best practices for AWS. These industry-accepted best practices go beyond the high-level security guidance already available in that they provide you with clear, step-by-step implementation and assessment procedures.

For more information, see the [CIS AWS Foundations Benchmark blog posts](#) on the *AWS Security Blog*.

Difference between CIS Benchmarks and CIS Controls

CIS Benchmarks are security best practice guidelines that are specific to vendor products. Ranging from operating systems to cloud services and networks devices, the settings that are applied from a benchmark protect the specific systems that your organization use. *CIS Controls* are foundational best practice guidelines for organization-level systems to follow to help protect against known cyberattack vectors.

Examples

- CIS Benchmarks are prescriptive. They typically reference a specific setting that can be reviewed and set in the vendor product.

Example: CIS Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 Ensure MFA is enabled for the "root user" account

This recommendation provides prescriptive guidance on how to check for this and how to set this on the root account for the AWS environment.

- CIS Controls are for your organization as a whole. They aren't specific to only one vendor product.

Example: CIS Controls v7.1 - Sub-Control 4.5 Use Multi-Factor Authentication for All Administrative Access

This control describes what's expected to be applied within your organization. It doesn't describe how you should apply it for the systems and workloads that you're running (regardless of where they are).

Using these frameworks to support your audit preparation

You can use the CIS AWS Foundations Benchmark v1.2 frameworks in AWS Audit Manager to help you prepare for CIS audits. You can also customize these frameworks and their controls to support internal audits with specific requirements.

Using the frameworks as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the CIS framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.2.0, Level 1	33	3	4	<ul style="list-style-type: none">Amazon Elastic Compute CloudAWS CloudTrailAWS Identity and Access ManagementAWS Security Hub
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.2.0, Level 1 and 2	45	4	4	<ul style="list-style-type: none">Amazon Elastic Compute CloudAWS CloudTrailAWS Identity and Access ManagementAWS Security Hub

The controls in these frameworks aren't intended to verify if your systems are compliant with the CIS standard. Moreover, they can't guarantee that you'll pass a CIS audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find these frameworks under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using these frameworks, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from these standard frameworks, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the CIS Benchmarks. If you need to edit the list of services in scope for these frameworks, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize these frameworks to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

Prerequisites for using these frameworks

Many controls in the CIS AWS Foundations Benchmark v1.2 frameworks use AWS Config as a data source type. To support these controls, you must [enable AWS Config](#) on all accounts in each AWS Region where you enabled Audit Manager. You must also make sure that specific AWS Config rules are enabled, and that these rules are configured correctly.

The following AWS Config rules and parameters are required to collect the correct evidence and capture an accurate compliance status for the CIS AWS Foundations Benchmark v1.2. For instructions on how to enable or configure a rule, see [Working with AWS Config Managed Rules](#).

Required AWS Config rule	Required parameters
ACCESS_KEYS_ROTATED	maxAccessKeyAge <ul style="list-style-type: none"> The maximum number of days without rotation. Type: Int Default: 90 days Compliance requirement: A maximum of 90 days
CLOUD_TRAIL_CLOUD_WATCH_LOGGING_INTEGRITY	Not applicable
CLOUD_TRAIL_ENCRYPTION_ENABLED	Not applicable
CLOUD_TRAIL_LOG_FILE_VALIDATION	Not applicable
CMK_BACKING_KEY_ROTATION_ENABLED	Not applicable
IAM_PASSWORD_POLICY	MaxPasswordAge (Optional) <ul style="list-style-type: none"> The number of days before password expiration. Type: int Default: 90 Compliance requirement: A maximum of 90 days
IAM_PASSWORD_POLICY	MinimumPasswordLength (Optional) <ul style="list-style-type: none"> The minimum length of the password. Type: int Default: 14 Compliance requirement: A minimum of 14 characters
IAM_PASSWORD_POLICY	PasswordReusePrevention (Optional) <ul style="list-style-type: none"> The number of passwords before allowing reuse. Type: int Default: 24 Compliance requirement: A minimum of 24 passwords before reuse
IAM_PASSWORD_POLICY	RequireLowercaseCharacters (Optional) <ul style="list-style-type: none"> Require at least one lowercase character in password. Type: Boolean Default: True Compliance requirement: At least one lowercase character
IAM_PASSWORD_POLICY	RequireNumbers (Optional) <ul style="list-style-type: none"> Require at least one number in password. Type: Boolean Default: True Compliance requirement: At least one number character
IAM_PASSWORD_POLICY	RequireSymbols (Optional) <ul style="list-style-type: none"> Require at least one symbol in password.

Required AWS Config rule	Required parameters
	<ul style="list-style-type: none"> • Type: Boolean • Default: True • Compliance requirement: At least one symbol character
<u>IAM_PASSWORD_POLICY</u>	RequireUppercaseCharacters (Optional) <ul style="list-style-type: none"> • Require at least one uppercase character in password. • Type: Boolean • Default: True • Compliance requirement: At least one uppercase character
<u>IAM_POLICY_IN_USE</u>	policyARN <ul style="list-style-type: none"> • An IAM policy ARN to be checked. • Type: String • Compliance requirement: Creates an IAM role for managing incidents with AWS. policyUsageType (Optional) <ul style="list-style-type: none"> • Specifies whether you expect the policy to be attached to a user, group, or role. • Type: String • Valid values: IAM_USER IAM_GROUP IAM_ROLE ANY • Default value: ANY • Compliance requirement: Attach the trust policy to the created IAM role
<u>IAM_POLICY_NO_STATEMENTS_WITHOUT_EFFECTIVE_PERMISSIONS</u>	Not applicable
<u>IAM_ROOT_ACCESS_KEY_CHECK</u>	Not applicable
<u>IAM_USER_NO_POLICIES_CHECK</u>	Not applicable
<u>IAM_USER_UNUSED_CREDENTIALS</u>	maxCredentialUsageAge <ul style="list-style-type: none"> • The maximum number of days that a credential can't be used. • Type: Int • Default: 90 days • Compliance requirement: 90 days or greater
<u>INCOMING_SSH_DISABLED</u>	Not applicable
<u>MFA_ENABLED_FOR_IAM_CONSOLE</u>	Not applicable
<u>MULTI_REGION_CLOUD_TRAIL_ENABLING</u>	Not applicable

Required AWS Config rule	Required parameters
RESTRICTED_INCOMING_TRAFFIC	<p>blockedPort1 (Optional)</p> <ul style="list-style-type: none"> The blocked TCP port number. Type: int Default: 20 Compliance requirement: Ensure that no security groups allow ingress on blocked ports <p>blockedPort2 (Optional)</p> <ul style="list-style-type: none"> The blocked TCP port number. Type: int Default: 21 Compliance requirement: Ensure that no security groups allow ingress on blocked ports <p>blockedPort3 (Optional)</p> <ul style="list-style-type: none"> The blocked TCP port number. Type: int Default: 3389 Compliance requirement: Ensure that no security groups allow ingress on blocked ports <p>blockedPort4 (Optional)</p> <ul style="list-style-type: none"> The blocked TCP port number. Type: int Default: 3306 Compliance requirement: Ensure that no security groups allow ingress on blocked ports <p>blockedPort5 (Optional)</p> <ul style="list-style-type: none"> The blocked TCP port number. Type: int Default: 4333 Compliance requirement: Ensure that no security groups allow ingress on blocked ports
ROOT_ACCOUNT_HARDWARE_MFA	Not applicable
ROOT_ACCOUNT_MFA_ENABLED	Not applicable
S3_BUCKET_LOGGING_ENABLED	<p>targetBucket (Optional)</p> <ul style="list-style-type: none"> The target S3 bucket for storing server access logs. Type: String Compliance requirement: Enable logging <p>targetPrefix (Optional)</p> <ul style="list-style-type: none"> The prefix of the S3 bucket for storing server access logs. Type: String Compliance requirement: Identify the S3 bucket for CloudTrail logging
S3_BUCKET_PUBLIC_READ_PROHIBITED	Not applicable
VPC_DEFAULT_SECURITY_GROUP_CLOUDTRAIL	Not applicable

Required AWS Config rule	Required parameters
VPC_FLOW_LOGS_ENABLED	trafficType (Optional) <ul style="list-style-type: none">The trafficType of the flow logs.Type: StringCompliance requirement: Flow logging is enabled

More CIS resources

- [The CIS AWS Foundations Benchmark v1.2.0](#)
- [CIS AWS Foundations Benchmark blog posts](#) on the *AWS Security Blog*

CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0

AWS Audit Manager provides two prebuilt frameworks that support the CIS AWS Foundations Benchmark v1.3:

- *CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0, Level 1*
- *CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0, Level 1 and 2*

Note

For information about CIS AWS Foundations Benchmark v1.2.0, and the AWS Audit Manager frameworks that support this version of the benchmark, see [CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.2.0 \(p. 145\)](#).

Topics

- [What is CIS? \(p. 151\)](#)
- [Using these frameworks to support your audit preparation \(p. 152\)](#)
- [More CIS resources \(p. 153\)](#)

What is CIS?

The *Center for Internet Security (CIS)* developed the [CIS AWS Foundations Benchmark](#) v1.3.0, a set of security configuration best practices for AWS. These industry-accepted best practices go beyond the high-level security guidance already available in that they provide AWS users with clear, step-by-step implementation and assessment procedures.

For more information, see the [CIS AWS Foundations Benchmark blog posts](#) on the *AWS Security Blog*.

CIS AWS Foundations Benchmark v1.3.0 provides guidance for configuring security options for a subset of AWS services with an emphasis on foundational, testable, and architecture agnostic settings. Some of the specific Amazon Web Services in scope for this document include the following:

- 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)

Difference between CIS Benchmarks and CIS Controls

The *CIS Benchmarks* are security best practice guidelines that are specific to vendor products. Ranging from operating systems to cloud services and networks devices, the settings that are applied from a benchmark protect the systems that your organization uses. The *CIS Controls* are foundational best practice guidelines for your organization to follow to help protect from known cyberattack vectors.

Examples

- CIS Benchmarks are prescriptive. They typically reference a specific setting that can be reviewed and set in the vendor product.

Example: CIS Amazon Web Services Foundations Benchmark v1.3.0 - 1.5 Ensure MFA is enabled for the "root user" account

This recommendation provides prescriptive guidance on how to check for this and how to set this on the root account for the AWS environment.

- CIS Controls are for your organization as a whole, and aren't specific to only one vendor product.

Example: CIS Controls v7.1 - Sub-Control 4.5 Use Multi-Factor Authentication for All Administrative Access

This control describes what's expected to be applied within your organization, but not how you should apply it for the systems and workloads that you're running (regardless of where they are).

Using these frameworks to support your audit preparation

You can use the CIS AWS Foundations Benchmark v1.3 frameworks in AWS Audit Manager to help you prepare for CIS audits. You can also customize these frameworks and their controls to support internal audits with specific requirements.

Using the frameworks as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the CIS framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0, Level 1	33	5	6	<ul style="list-style-type: none">• Amazon CloudWatch• Amazon Elastic Compute Cloud• AWS Config• AWS CloudTrail

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
				<ul style="list-style-type: none"> • AWS Identity and Access Management • AWS Security Hub
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0, Level 1 and 2	49	6	6	<ul style="list-style-type: none"> • Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

Tip

To review a list of the AWS Config rules that are used as data source mappings for these standard frameworks, download the following files:

- [AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.3.0-Level-1.zip](#)
- [AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.3.0,Level1-and-2.zip](#)

The controls in these frameworks aren't intended to verify if your systems are compliant with the CIS standard. Moreover, they can't guarantee that you'll pass a CIS audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find these frameworks under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using these frameworks, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from these standard frameworks, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the CIS Benchmarks. If you need to edit the list of services in scope for these frameworks, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize these frameworks to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More CIS resources

- [CIS AWS Foundations Benchmark blog posts](#) on the [AWS Security Blog](#)

CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4.0

AWS Audit Manager provides two prebuilt standard frameworks that support the Center for Internet Security's (CIS) AWS Foundations Benchmark v1.4.0:

- *CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4.0, Level 1*
- *CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4.0, Level 1 and 2*

Note

- For information about the Audit Manager frameworks that support v1.2.0, see [CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.2.0 \(p. 145\)](#).
- For information about the Audit Manager frameworks that support v1.3.0, see [CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0 \(p. 151\)](#).

Topics

- [What is the CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4.0? \(p. 154\)](#)
- [Using these frameworks to support your audit preparation \(p. 155\)](#)
- [More CIS resources \(p. 156\)](#)

What is the CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4.0?

The CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.4.0, Level 1 and 2 provides prescriptive guidance for configuring security options for a subset of Amazon Web Services. It has an emphasis on foundational, testable, and architecture agnostic settings. Some of the specific Amazon Web Services in scope for this document include the following:

- 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

Difference between CIS Benchmarks and CIS Controls

The *CIS Benchmarks* are security best practice guidelines that are specific to vendor products. Ranging from operating systems to cloud services and networks devices, the settings that are applied from a benchmark protect the systems that are being used. The *CIS Controls* are foundational best practice guidelines for your organization to follow to help protect from known cyberattack vectors.

Examples

- CIS Benchmarks are prescriptive. They typically reference a specific setting that can be reviewed and set in the vendor product.

Example: CIS Amazon Web Services Foundations Benchmark v1.4.0 - 1.5 Ensure MFA is enabled for the "root user" account

This recommendation provides prescriptive guidance on how to check for this and how to set this on the root account for the AWS environment.

- CIS Controls are for your organization as a whole, and aren't specific to only one vendor product.

Example: CIS Controls v7.1 - Sub-Control 4.5 Use Multi-Factor Authentication for All Administrative Access

This control describes what's expected to be applied within your organization. However, it doesn't describe how to apply it for the systems and workloads that you're running, regardless of where they are.

Using these frameworks to support your audit preparation

You can use the CIS AWS Foundations Benchmark v1.4.0 frameworks in AWS Audit Manager to help you prepare for CIS audits. You can also customize these frameworks and their controls to support internal audits with specific requirements.

Using the frameworks as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the CIS framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4.0, Level 1	32	6	7	<ul style="list-style-type: none">• Amazon Elastic Compute Cloud• Amazon CloudWatch• AWS CloudTrail• AWS Config• AWS Identity and Access Management
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4.0, Level 1 and 2	50	8	7	<ul style="list-style-type: none">• Amazon Elastic Compute Cloud• Amazon CloudWatch• AWS CloudTrail• AWS Config

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
				<ul style="list-style-type: none">• AWS Identity and Access Management• AWS Security Hub

Tip

To review a list of the AWS Config rules that are used as data source mappings for these standard frameworks, download the following files:

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

The controls in these frameworks aren't intended to verify if your systems are compliant with the CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4.0 standard. Moreover, they can't guarantee that you'll pass a CIS audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find these frameworks under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using these frameworks, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from these standard frameworks, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the CIS Benchmarks. If you need to edit the list of services in scope for these frameworks, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize these frameworks to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More CIS resources

- [CIS Benchmarks](#) from the *Center for Internet Security*
- [CIS AWS Foundations Benchmark blog posts](#) on the *AWS Security Blog*

CIS Controls v7.1 Implementation Group 1

AWS Audit Manager provides a prebuilt framework that supports Center for Internet Security (CIS) Controls v7.1 Implementation Group 1.

Note

For information about CIS Controls v8 IG1 and the AWS Audit Manager framework that supports this standard, see [CIS Controls v8 Implementation Group 1 \(p. 158\)](#).

AWS Audit Manager provides a prebuilt framework that supports the *Center for Internet Security (CIS)* to assist you with your audit preparation.

Topics

- [What are CIS controls? \(p. 157\)](#)
- [Using this framework to support your audit preparation \(p. 157\)](#)
- [More CIS resources \(p. 158\)](#)

What are CIS controls?

The CIS Controls are a prioritized set of actions that collectively form a defense-in-depth set of best practices. These best practices mitigate the most common attacks against systems and networks. *Implementation Group 1* is generally defined for an organization with limited resources and cybersecurity expertise that are available to implement Sub-Controls.

Difference between CIS Controls and CIS Benchmarks

The CIS Controls are foundational best practice guidelines that an organization can follow to have protection from known cyberattack vectors. The CIS Benchmarks are security best practice guidelines specific to vendor products. Ranging from operating systems to cloud services and network devices, the settings that are applied from a Benchmark protect the systems that are being used.

Examples

- *CIS Benchmarks* are prescriptive. They typically reference a specific setting that can be reviewed and set in the vendor product.
 - **Example:** CIS Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 Ensure MFA is enabled for the "root user" account.
 - This recommendation provides prescriptive guidance on how to check for this and how to set this on the root account for the AWS environment.
- *CIS Controls* are for your organization as a whole and aren't specific to only one vendor product.
 - **Example:** CIS Controls v7.1 - Sub-Control 4.5 Use Multi-Factor Authentication for All Administrative Access
 - This control describes what's expected to be applied within your organization. However, it doesn't tell you how you should apply it for the systems and workloads that you're running (regardless of where they are).

Using this framework to support your audit preparation

You can use the *CIS Controls v7.1 IG1* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to CIS requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the CIS Controls v7.1 IG1 framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The CIS Controls v7.1 IG1 framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
CIS Controls v7.1 IG1	21	22	16	<ul style="list-style-type: none">• Amazon Elastic Compute Cloud

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
				<ul style="list-style-type: none">• AWS CloudTrail• AWS Config• AWS Identity and Access Management

Tip

To review the AWS Config rules that are used as data source mappings in this standard framework, download the [AuditManager_ConfigDataSourceMappings_CIS-Controls-v7.1-IG1.zip](#) file.

The controls in this framework aren't intended to verify if your systems are compliant with CIS Controls. Moreover, they can't guarantee that you'll pass a CIS audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find this framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the CIS Controls. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More CIS resources

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

CIS Controls v8 Implementation Group 1

AWS Audit Manager provides a prebuilt standard framework that supports the Center for Internet Security (CIS) Controls v8 Implementation Group 1.

Note

For information about CIS Controls v7.1 IG1 and the AWS Audit Manager framework that supports this standard, see [CIS Controls v7.1 Implementation Group 1 \(p. 156\)](#).

Topics

- [What are CIS Controls? \(p. 159\)](#)
- [Using this framework to support your audit preparation \(p. 159\)](#)
- [More CIS resources \(p. 160\)](#)

What are CIS Controls?

The CIS Critical Security Controls (CIS Controls) are a prioritized set of safeguards to mitigate the most prevalent cyberattacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks. CIS Controls v8 has been enhanced to keep up with modern systems and software. Movement to cloud-based computing, virtualization, mobility, outsourcing, work-from-home, and changing attacker tactics prompted the update. This update supports the security of enterprises as they move to both fully cloud and hybrid environments.

Difference between CIS Controls and CIS Benchmarks

The CIS Controls are foundational best practice guidelines that an organization can follow to have protection from known cyberattack vectors. The CIS Benchmarks are security best practice guidelines specific to vendor products. Ranging from operating systems to cloud services and network devices, the settings that are applied from a Benchmark protect the systems that are being used.

Examples

- *CIS Benchmarks* are prescriptive. They typically reference a specific setting that can be reviewed and set in the vendor product.
 - **Example:** CIS Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 Ensure MFA is enabled for the "root user" account.
 - This recommendation provides prescriptive guidance on how to check for this and how to set this on the root account for the AWS environment.
- *CIS Controls* are for your organization as a whole and aren't specific to only one vendor product.
 - **Example:** CIS Controls v7.1 - Sub-Control 4.5 Use Multi-Factor Authentication for All Administrative Access
 - This control describes what's expected to be applied within your organization. However, it doesn't tell you how you should apply it for the systems and workloads that you're running (regardless of where they are).

Using this framework to support your audit preparation

You can use the *CIS Controls v8 IG1* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to CIS requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the CIS Controls v8 framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The CIS Controls v8 framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
CIS Controls v8 IG1	25	31	15	<ul style="list-style-type: none">• Amazon Elastic Compute Cloud• AWS Config

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
				<ul style="list-style-type: none">• AWS Identity and Access Management• AWS License Manager

Tip

To review the AWS Config rules that are used as data source mappings in this standard framework, download the [AuditManager_ConfigDataSourceMappings_CIS-Controls-v8-IG1.zip](#) file.

The controls in this framework aren't intended to verify if your systems are compliant with CIS Controls. Moreover, they can't guarantee that you'll pass a CIS audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find this framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the CIS Controls. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More CIS resources

- [CIS Controls v8](#)

FedRAMP Moderate Baseline

AWS Audit Manager provides a *FedRAMP Moderate Baseline* framework to assist you with your audit preparation.

Topics

- [What is FedRAMP? \(p. 160\)](#)
- [Using this framework to support your audit preparation \(p. 161\)](#)
- [More FedRAMP resources \(p. 162\)](#)

What is FedRAMP?

The Federal Risk and Authorization Management Program (FedRAMP) was established in 2011. It provides a cost-effective, risk-based approach for the adoption and use of cloud services by the U.S. federal government. FedRAMP empowers federal agencies to use modern cloud technologies, with an emphasis on the security and protection of federal information.

For more information about the FedRAMP moderate baseline controls, see the [FedRAMP Moderate Security Test Case Procedures Template](#).

Using this framework to support your audit preparation

You can use the *FedRAMP Moderate Baseline* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to FedRAMP requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The FedRAMP Moderate Baseline framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
FedRAMP Moderate Baseline	303	908	325	<ul style="list-style-type: none">Amazon Elastic Compute CloudAWS ConfigAWS Identity and Access Management

Tip

To review the AWS Config rules that are used as data source mappings in this standard framework, download the [AuditManager_ConfigDataSourceMappings_FedRAMP-Moderate-Baseline.zip](#) file.

The controls in this framework aren't intended to verify if your systems are compliant with FedRAMP. Moreover, they can't guarantee that you'll pass a FedRAMP audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find this framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the FedRAMP Moderate Baseline. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More FedRAMP resources

- [AWS Compliance page for FedRAMP](#)
- [AWS FedRAMP blog posts](#)

General Data Protection Regulation (GDPR)

AWS Audit Manager provides a prebuilt standard framework that supports the General Data Protection Regulation (GDPR). By default, this framework contains only manual controls. These manual controls don't collect evidence automatically. However, if you want to automate evidence collection for some controls under GDPR, you can use the custom control feature in AWS Audit Manager. For more information, see [Using this framework to support your audit preparation \(p. 162\)](#).

Topics

- [What is the General Data Protection Regulation \(GDPR\)? \(p. 162\)](#)
- [Using this framework to support your audit preparation \(p. 162\)](#)
- [More GDPR resources \(p. 180\)](#)

What is the General Data Protection Regulation (GDPR)?

The *General Data Protection Regulation (GDPR)* is a new European privacy law that became enforceable on May 25, 2018. The GDPR replaces the EU Data Protection Directive, also known as [Directive 95/46/EC](#). It's intended to harmonize data protection laws throughout the European Union (EU). It does this by applying a single data protection law that's binding throughout each EU member state.

The GDPR applies to all organizations that are established in the EU and to organizations (no matter whether they were established in the EU) that process the personal data of EU data subjects in connection with either the offering of goods or services to data subjects in the EU or the monitoring of behavior that takes place within the EU. Personal data is any information that relates to an identified or identifiable natural person.

You can find the GDPR framework in the framework library page of AWS Audit Manager. For more information, see the [General Data Protection Regulation \(GDPR\) Center](#).

Using this framework to support your audit preparation

You can use the *GDPR* framework in AWS Audit Manager to help you prepare for audits.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
GDPR	0	371	10	None

You can find the GDPR framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager. Because this standard framework contains manual controls only, no AWS services are in scope.

Note

If you want to automate evidence collection for GDPR, you can use Audit Manager to [create your own custom controls](#) for GDPR. The following table provides recommendations on the AWS data

sources that you can map to GDPR requirements in your custom controls. Although some of the following data sources are mapped to multiple controls, keep in mind that you're charged only once for each resource assessment.

The following recommendations use AWS Config and AWS Security Hub as data sources. To successfully collect evidence from these data sources, make sure that you do the following:

- Confirm that you've followed the instructions to [enable and set up AWS Config and AWS Security Hub](#) in your AWS account.
- Confirm that you've included both AWS Config and Security Hub as services in scope. To review the list of services in scope for your assessment, see [Review an assessment, AWS services tab](#). To edit this list, see [Edit AWS services in scope](#).

After you've set up both services in this way, Audit Manager collects evidence each time an evaluation occurs for the specified AWS Config rule or Security Hub control.

Control name	Control set	Recommended control data source mapping
Article 25 Data protection by design and by default. ¹	Chapter 4 - Controller and Processor	<p>You can create a custom control in AWS Audit Manager that supports this GDPR control.</p> <p>When you specify the control details, enter the following under Testing information:</p> <ul style="list-style-type: none"> • Show all root account events over term • AWS CloudTrail bucket not public • Show all policies with an Allow:<code>* : *</code> and list all principals and services using those policies <p>When you set up the control data sources, we recommend that you include all of the following as data sources:</p> <p>Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings:</p> <ul style="list-style-type: none"> • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY <p>Choose AWS Security Hub as the data source type, and select the following Security Hub controls as data source mappings:</p> <ul style="list-style-type: none"> • 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)

Control name	Control set	Recommended control data source mapping
		<ul style="list-style-type: none">• 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 (Config.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)• Config.1

Control name	Control set	Recommended control data source mapping
Article 25 Data protection by design and by default. ²	Chapter 4 - Controller and Processor	<p>You can create a custom control in AWS Audit Manager that supports this GDPR control.</p> <p>When you specify the control details, enter the following under Testing information:</p> <ul style="list-style-type: none"> • Show all root account events over term • AWS CloudTrail bucket not public • Show all policies with an Allow: * : * and list all principals and services using those policies <p>When you set up the control data sources, we recommend that you include all of the following as data sources:</p> <p>Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings:</p> <ul style="list-style-type: none"> • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY <p>Choose AWS Security Hub as the data source type, and select the following Security Hub controls as data source mappings:</p> <ul style="list-style-type: none"> • 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) • 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)

Control name	Control set	Recommended control data source mapping
		<ul style="list-style-type: none">• 2.3 (CloudTrail.6)• 2.4 (CloudTrail.5)• 2.5 (Config.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)• Config.1

Control name	Control set	Recommended control data source mapping
Article 25 Data protection by design and by default. ³	Chapter 4 - Controller and Processor	<p>You can create a custom control in AWS Audit Manager that supports this GDPR control.</p> <p>When you specify the control details, enter the following under Testing information:</p> <ul style="list-style-type: none"> • Show all root account events over term • AWS CloudTrail bucket not public • Show all policies with an Allow: * : * and list all principals and services using those policies <p>When you set up the control data sources, we recommend that you include all of the following as data sources:</p> <p>Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings:</p> <ul style="list-style-type: none"> • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY <p>Choose AWS Security Hub as the data source type, and select the following Security Hub controls as data source mappings:</p> <ul style="list-style-type: none"> • 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) • 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)

Control name	Control set	Recommended control data source mapping
		<ul style="list-style-type: none"> • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.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) • Config.1
Article 30 Records of processing activities.1	Chapter 4 - Controller and Processor	<p>You can create a custom control in AWS Audit Manager that supports this GDPR control.</p> <p>When you specify the control details, enter the following under Testing information:</p> <ul style="list-style-type: none"> • Show all root account events over term <p>When you set up the control data sources, we recommend that you include all of the following as data sources:</p> <p>Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings:</p> <ul style="list-style-type: none"> • 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 <p>Choose AWS Security Hub as the data source type, and select the following Security Hub control as a data source mapping:</p> <ul style="list-style-type: none"> • Config.1

Control name	Control set	Recommended control data source mapping
Article 30 Records of processing activities. ²	Chapter 4 - Controller and Processor	<p>You can create a custom control in AWS Audit Manager that supports this GDPR control.</p> <p>When you specify the control details, enter the following under Testing information:</p> <ul style="list-style-type: none"> • Show all root account events over term <p>When you set up the control data sources, we recommend that you include all of the following as data sources:</p> <p>Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings:</p> <ul style="list-style-type: none"> • 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 <p>Choose AWS Security Hub as the data source type, and select the following Security Hub control as a data source mapping:</p> <ul style="list-style-type: none"> • Config.1

Control name	Control set	Recommended control data source mapping
Article 30 Records of processing activities. ³	Chapter 4 - Controller and Processor	<p>You can create a custom control in AWS Audit Manager that supports this GDPR control.</p> <p>When you specify the control details, enter the following under Testing information:</p> <ul style="list-style-type: none"> • Show all root account events over term • AWS CloudTrail bucket not public • Show all policies with an Allow: * : * and list all principals and services using those policies <p>When you set up the control data sources, we recommend that you include all of the following as data sources:</p> <p>Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings:</p> <ul style="list-style-type: none"> • 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 <p>Choose AWS Security Hub as the data source type, and select the following Security Hub control as a data source mapping:</p> <ul style="list-style-type: none"> • Config.1

Control name	Control set	Recommended control data source mapping
Article 30 Records of processing activities. ⁴	Chapter 4 - Controller and Processor	<p>You can create a custom control in AWS Audit Manager that supports this GDPR control.</p> <p>When you specify the control details, enter the following under Testing information:</p> <ul style="list-style-type: none"> • Show all root account events over term • AWS CloudTrail bucket not public • Show all policies with an Allow: * : * and list all principals and services using those policies <p>When you set up the control data sources, we recommend that you include all of the following as data sources:</p> <p>Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings:</p> <ul style="list-style-type: none"> • 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 <p>Choose AWS Security Hub as the data source type, and select the following Security Hub control as a data source mapping:</p> <ul style="list-style-type: none"> • Config.1

Control name	Control set	Recommended control data source mapping
Article 30 Records of processing activities. ⁵	Chapter 4 - Controller and Processor	<p>You can create a custom control in AWS Audit Manager that supports this GDPR control.</p> <p>When you specify the control details, enter the following under Testing information:</p> <ul style="list-style-type: none"> • Show all root account events over term <p>When you set up the control data sources, we recommend that you include all of the following as data sources:</p> <p>Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings:</p> <ul style="list-style-type: none"> • 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 <p>Choose AWS Security Hub as the data source type, and select the following Security Hub control as a data source mapping:</p> <ul style="list-style-type: none"> • Config.1

Control name	Control set	Recommended control data source mapping
Article 32 Security of processing.1	Chapter 4 - Controller and Processor	<p>You can create a custom control in AWS Audit Manager that supports this GDPR control.</p> <p>When you specify the control details, enter the following under Testing information:</p> <ul style="list-style-type: none"> • Show data at rest encryption for all services • Show data in transit encryption for all services • MFA Delete enabled for Amazon S3 • All Amazon Inspector scans • Show all instances that are not Amazon Inspector enabled • Show all load balancers that are listening on HTTPS (SSL) • AWS CloudTrail encrypted at rest • Amazon CloudWatch alerts for AWS Config displaying all changes and all commented settings • All root activity <p>When you set up the control data sources, we recommend that you include all of the following as data sources:</p> <p>Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings:</p> <ul style="list-style-type: none"> • 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 • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN

Control name	Control set	Recommended control data source mapping
		<ul style="list-style-type: none">• WAF_CLASSIC_LOGGING_ENABLED• WAFV2_LOGGING_ENABLED• ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK• ELB_ACM_CERTIFICATE_REQUIRED• ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK• REDSHIFT_REQUIRE_TLS_SSL• CLOUDFRONT_VIEWER_POLICY_HTTPS• ALB_HTTP_DROP_INVALID_HEADER_ENABLED• ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK• ELB_TLS_HTTPS_LISTENERS_ONLY• ACM_CERTIFICATE_EXPIRATION_CHECK• API_GW_CACHE_ENABLED_AND_ENCRYPTED

Control name	Control set	Recommended control data source mapping
Article 32 Security of processing.2	Chapter 4 - Controller and Processor	<p>You can create a custom control in AWS Audit Manager that supports this GDPR control.</p> <p>When you specify the control details, enter the following under Testing information:</p> <ul style="list-style-type: none"> • Show data at rest encryption for all services • Show data in transit encryption for all services • MFA Delete enabled for Amazon S3 • All Amazon Inspector scans • Show all instances that aren't Amazon Inspector enabled • Show all load balancers that are listening on HTTPS (SSL) • AWS CloudTrail encrypted at rest • Amazon CloudWatch alerts for AWS Config displaying all changes and all commented settings • All root activity <p>When you set up the control data sources, we recommend that you include all of the following as data sources:</p> <p>Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings:</p> <ul style="list-style-type: none"> • 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 • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN

Control name	Control set	Recommended control data source mapping
		<ul style="list-style-type: none">• WAF_CLASSIC_LOGGING_ENABLED• WAFV2_LOGGING_ENABLED• ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK• ELB_ACM_CERTIFICATE_REQUIRED• ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK• REDSHIFT_REQUIRE_TLS_SSL• CLOUDFRONT_VIEWER_POLICY_HTTPS• ALB_HTTP_DROP_INVALID_HEADER_ENABLED• ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK• ELB_TLS_HTTPS_LISTENERS_ONLY• ACM_CERTIFICATE_EXPIRATION_CHECK• API_GW_CACHE_ENABLED_AND_ENCRYPTED

Control name	Control set	Recommended control data source mapping
Article 32 Security of processing.3	Chapter 4 - Controller and Processor	<p>You can create a custom control in AWS Audit Manager that supports this GDPR control.</p> <p>When you specify the control details, enter the following under Testing information:</p> <ul style="list-style-type: none"> • Show data at rest encryption for all services • Show data in transit encryption for all services • MFA Delete enabled for Amazon S3 • All Amazon Inspector scans • Show all instances that aren't Amazon Inspector enabled • Show all load balancers that are listening on HTTPS (SSL) • AWS CloudTrail encrypted at rest • Amazon CloudWatch alerts for AWS Config displaying all changes and all commented settings • All root activity <p>When you set up the control data sources, we recommend that you include all of the following as data sources:</p> <p>Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings:</p> <ul style="list-style-type: none"> • 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 • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN

Control name	Control set	Recommended control data source mapping
		<ul style="list-style-type: none">• WAF_CLASSIC_LOGGING_ENABLED• WAFV2_LOGGING_ENABLED• ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK• ELB_ACM_CERTIFICATE_REQUIRED• ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK• REDSHIFT_REQUIRE_TLS_SSL• CLOUDFRONT_VIEWER_POLICY_HTTPS• ALB_HTTP_DROP_INVALID_HEADER_ENABLED• ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK• ELB_TLS_HTTPS_LISTENERS_ONLY• ACM_CERTIFICATE_EXPIRATION_CHECK• API_GW_CACHE_ENABLED_AND_ENCRYPTED

Control name	Control set	Recommended control data source mapping
Article 32 Security of processing.4	Chapter 4 - Controller and Processor	<p>You can create a custom control in AWS Audit Manager that supports this GDPR control.</p> <p>When you specify the control details, enter the following under Testing information:</p> <ul style="list-style-type: none"> • Show data at rest encryption for all services • Show data in transit encryption for all services • MFA Delete enabled for Amazon S3 • All Amazon Inspector scans • Show all instances that aren't Amazon Inspector enabled • Show all load balancers that are listening on HTTPS (SSL) • AWS CloudTrail encrypted at rest • Amazon CloudWatch alerts for AWS Config displaying all changes and all commented settings • All root activity <p>When you set up the control data sources, we recommend that you include all of the following as data sources:</p> <p>Choose AWS Config as the data source type, and select the following AWS Config managed rules as data source mappings:</p> <ul style="list-style-type: none"> • 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 • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN

Control name	Control set	Recommended control data source mapping
		<ul style="list-style-type: none">• WAF_CLASSIC_LOGGING_ENABLED• WAFV2_LOGGING_ENABLED• ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK• ELB_ACM_CERTIFICATE_REQUIRED• ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK• REDSHIFT_REQUIRE_TLS_SSL• CLOUDFRONT_VIEWER_POLICY_HTTPS• ALB_HTTP_DROP_INVALID_HEADER_ENABLED• ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK• ELB_TLS_HTTPS_LISTENERS_ONLY• ACM_CERTIFICATE_EXPIRATION_CHECK• API_GW_CACHE_ENABLED_AND_ENCRYPTED

After you create your new custom controls for GDPR, you can add them to a custom GDPR framework. For more information, see [Creating a custom framework \(p. 110\)](#) and [Editing a custom framework \(p. 114\)](#). You can then create an assessment from the custom GDPR framework. This way, AWS Audit Manager can collect evidence automatically for the custom controls that you added. For instructions on how to create an assessment from a framework, see [Creating an assessment \(p. 50\)](#).

More GDPR resources

- [General Data Protection Regulation \(GDPR\) Center](#)
- [AWS GDPR blog posts](#)

Gramm-Leach-Bliley Act

AWS Audit Manager provides a prebuilt framework that supports the Gramm-Leach-Bliley Act (GLBA).

Topics

- [What is the Gramm-Leach-Bliley Act \(GLBA\)? \(p. 180\)](#)
- [Using this framework to support your audit preparation \(p. 180\)](#)

What is the Gramm-Leach-Bliley Act (GLBA)?

The Gramm-Leach-Bliley Act (GLB Act or GLBA), also known as the Financial Service Modernization Act of 1999, is a federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals. The Act consists of three sections. The first is the Financial Privacy Rule, which regulates the collection and disclosure of private financial information. The second is the Safeguards Rule, which stipulates that financial institutions must implement security programs to protect such information. The third is the Pretexting provisions, which prohibit the practice of pretexting (accessing private information using false pretenses). The Act also requires financial institutions to give customers written privacy notices that explain their information-sharing practices.

Using this framework to support your audit preparation

You can use the *Gramm-Leach-Bliley Act (GLBA)* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These

controls are grouped into control sets according to GLBA requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the GLBA framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for a GLBA audit. In your assessment, you can specify the AWS accounts and services that you want to include in the scope of your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the GLBA framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The GLBA framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
Gramm-Leach-Bliley Act (GLBA)	4	110	16	<ul style="list-style-type: none">Amazon Elastic Compute CloudAWS CloudTrailAWS ConfigAWS Identity and Access ManagementAWS Security Hub

Tip

To review the AWS Config rules that are used as data source mappings in this standard framework, download the [AuditManager_ConfigDataSourceMappings_GLBA.zip](#) file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with the GLBA standard. Moreover, they can't guarantee that you'll pass a GLBA audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find the GLBA framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the GLBA. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

GxP 21 CFR part 11

AWS Audit Manager provides a prebuilt framework that supports GxP CFR part 11 regulations based on AWS best practices.

Note

For information about *GxP EU Annex 11* and the Audit Manager framework that supports it, see [GxP EU Annex 11 \(p. 183\)](#).

Topics

- [What is GxP CFR part 11? \(p. 182\)](#)
- [Using this framework to support your audit preparation \(p. 182\)](#)
- [More GxP resources \(p. 183\)](#)

What is GxP CFR part 11?

GxP refers to the regulations and guidelines that are applicable to life sciences organizations that make food and medical products. Medical products that fall under this include medicines, medical devices, and medical software applications. The overall intent of GxP requirements is to ensure that food and medical products are safe for consumers. It's also to ensure the integrity of data that's used to make product-related safety decisions.

The term GxP encompasses a broad range of compliance-related activities. These include Good Laboratory Practices (GLP), Good Clinical Practices (GCP), and Good Manufacturing Practices (GMP). Each of these different types of activities involves product-specific requirements that life sciences organizations must implement. This is based on the type of products the organizations make as well as the country where their products are sold. When life sciences organizations use computerized systems to perform certain GxP activities, they must ensure that the computerized GxP system is developed, validated, and operated appropriately for the intended use of the system.

For a comprehensive approach to using the AWS Cloud for GxP systems, see the [Considerations for Using AWS Products in GxP Systems](#) whitepaper.

Using this framework to support your audit preparation

You can use the *GxP 21 CFR Part 11* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to GxP requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the GxP 21 CFR Part 11 framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The GxP CFR Part 11 framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
GxP 21 CFR Part 11	13	14	7	<ul style="list-style-type: none">• AWS CloudTrail• AWS Config• AWS Identity and Access Management

Tip

To review the AWS Config rules that are used as data source mappings in this standard framework, download the [AuditManager_ConfigDataSourceMappings_GxP-21-CFR-Part-11.zip](#) file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with GxP regulations. Moreover, they can't guarantee that you'll pass a GxP audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find this framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the GxP CFR Part 11 framework. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More GxP resources

- [AWS Compliance page for GxP](#)
- [Considerations for Using AWS Products in GxP Systems](#)

GxP EU Annex 11

AWS Audit Manager provides a prebuilt framework that supports GxP EU Annex 11 regulations based on AWS best practices.

Note

For information about *GxP 21 CFR Part 11* and the Audit Manager framework that supports it, see [GxP 21 CFR part 11 \(p. 181\)](#).

Topics

- [What is GxP EU Annex 11? \(p. 183\)](#)
- [Using this framework to support your audit preparation \(p. 184\)](#)

What is GxP EU Annex 11?

The GxP EU Annex 11 framework is the European equivalent to the FDA 21 CFR part 11 framework in the United States. This annex applies to all forms of computerized systems that are used as part of Good Manufacturing Practices (GMP) regulated activities. A computerized system is a set of software and hardware components that together fulfill certain functionalities. The application should be validated and IT infrastructure should be qualified. Where a computerized system replaces a manual operation, there should be no resultant decrease in product quality, process control, or quality assurance. There should be no increase in the overall risk of the process.

Annex 11 is part of the European GMP guidelines and defines the terms of reference for computerized systems that are used by organizations in the pharmaceutical industry. Annex 11 functions as a checklist that enables the European regulatory agencies to establish the requirements for computerized systems that relate to pharmaceutical products and medical devices. The guidelines set by the Commission of the European Committees aren't that much distant from the FDA (21 CFR Part 11). Annex 11 defines the criteria for how electronic records and electronic signatures are considered to be managed.

Using this framework to support your audit preparation

You can use the *GxP EU Annex 11* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to GxP requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the *GxP EU Annex 11* framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The *GxP EU Annex 11* framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
GxP EU Annex 11	19	13	3	<ul style="list-style-type: none">Amazon CloudWatchAWS CloudTrailAWS ConfigAWS Identity and Access ManagementAWS Security Hub

Tip

To review the AWS Config rules that are used as data source mappings in this standard framework, download the [AuditManager_ConfigDataSourceMappings_GxP-EU-Annex-11.zip](#) file.

The controls in this framework aren't intended to verify if your systems are compliant with the *GxP EU Annex 11* requirements. Moreover, they can't guarantee that you'll pass a GxP audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find this framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the *GxP EU Annex 11* framework. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

Health Insurance Portability and Accountability Act (HIPAA) Security Rule 2003

AWS Audit Manager provides a prebuilt framework that supports HIPAA rules to assist you with your audit preparation.

Note

This framework was formerly named *HIPAA* in the framework library. On March 08, 2023, we updated this framework's name to *HIPAA Security Rule 2003* to differentiate it from *HIPAA Final Omnibus Security Rule 2013*.

For information about the HIPAA Final Omnibus Security Rule 2013 and the Audit Manager framework that supports this standard, see [Health Insurance Portability and Accountability Act \(HIPAA\) Final Omnibus Security Rule 2013 \(p. 187\)](#).

Topics

- [What is HIPAA and the HIPAA Security Rule 2003? \(p. 185\)](#)
- [Using this framework to support your audit preparation \(p. 185\)](#)
- [More HIPAA resources \(p. 186\)](#)

What is HIPAA and the HIPAA Security Rule 2003?

The *Health Insurance Portability and Accountability Act of 1996 (HIPAA)* is legislation that helps US workers to retain health insurance coverage when they change or lose jobs. The legislation also seeks to encourage electronic health records to improve the efficiency and quality of the US healthcare system through improved information sharing.

Along with increasing the use of electronic medical records, HIPAA includes provisions to protect the security and privacy of protected health information (PHI). PHI includes a very wide set of personally identifiable health and health-related data. This includes insurance and billing information, diagnosis data, clinical care data, and lab results such as images and test results.

The U.S. Department of Health and Human Services published a final [Security Rule](#) in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information.

HIPAA rules apply to covered entities. These include hospitals, medical services providers, employer-sponsored health plans, research facilities, and insurance companies that deal directly with patients and patient data. The HIPAA requirement to protect PHI also extends to business associates.

For more information about how HIPAA and HITECH protect health information, see the [Health Information Privacy](#) webpage from the U.S. Department of Health and Human Services.

A growing number of healthcare providers, payers, and IT professionals are using AWS utility-based cloud services to process, store, and transmit protected health information (PHI). AWS enables covered entities and their business associates subject to HIPAA to use the secure AWS environment to process, maintain, and store protected health information.

For instructions on how you can use AWS for the processing and storage of health information, see the [Architecting for HIPAA Security and Compliance on Amazon Web Services](#) whitepaper.

Using this framework to support your audit preparation

You can use the *HIPAA Security Rule 2003* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are

grouped into control sets according to HIPAA requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the HIPAA framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The HIPAA Security Rule 2003 framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
HIPAA Security Rule 2003	35	53	5	<ul style="list-style-type: none">Amazon Elastic Compute CloudAWS CloudTrailAWS ConfigAWS Identity and Access ManagementAWS Security Hub

Tip

To review the AWS Config rules that are used as data source mappings in this standard framework, download the [AuditManager_ConfigDataSourceMappings_HIPAA-Security-Rule-2003.zip](#) file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with the HIPAA standard. Moreover, they can't guarantee that you'll pass a HIPAA audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find this framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the HIPAA framework. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More HIPAA resources

- [Health Information Privacy](#) from the U.S. Department of Health and Human Service
- [The Security Rule](#) from the U.S. Department of Health and Human Service
- [Architecting for HIPAA Security and Compliance on Amazon Web Services](#)

- [AWS Compliance page for HIPAA](#)

Health Insurance Portability and Accountability Act (HIPAA) Final Omnibus Security Rule 2013

AWS Audit Manager provides a prebuilt framework that supports HIPAA rules to assist you with your audit preparation.

Note

For information about the HIPAA Security Rule 2003 and the AWS Audit Manager framework that supports this standard, see [Health Insurance Portability and Accountability Act \(HIPAA\) Security Rule 2003 \(p. 185\)](#).

Topics

- [What is HIPAA and the HIPAA Final Omnibus Security Rule? \(p. 187\)](#)
- [Using this framework to support your audit preparation \(p. 185\)](#)
- [More HIPAA resources \(p. 186\)](#)

What is HIPAA and the HIPAA Final Omnibus Security Rule?

The *Health Insurance Portability and Accountability Act of 1996 (HIPAA)* is legislation that helps US workers to retain health insurance coverage when they change or lose jobs. The legislation also seeks to encourage electronic health records to improve the efficiency and quality of the US healthcare system through improved information sharing.

Along with increasing the use of electronic medical records, HIPAA includes provisions to protect the security and privacy of protected health information (PHI). PHI includes a very wide set of personally identifiable health and health-related data. This includes insurance and billing information, diagnosis data, clinical care data, and lab results such as images and test results.

The HIPAA Final Omnibus Security Rule, which became effective in 2013, implements a number of updates to all of the previously passed rules. The modifications to the Security, Privacy, Breach Notification, and Enforcement Rules were intended to enhance confidentiality and security in data sharing.

HIPAA rules apply to covered entities. These include hospitals, medical services providers, employer-sponsored health plans, research facilities, and insurance companies that deal directly with patients and patient data. As part of the omnibus updates, many of the HIPAA rules that apply to covered entities also now apply to business associates.

For more information about how HIPAA and HITECH protect health information, see the [Health Information Privacy](#) webpage from the U.S. Department of Health and Human Services.

A growing number of healthcare providers, payers, and IT professionals are using AWS utility-based cloud services to process, store, and transmit protected health information (PHI). AWS enables covered entities and their business associates subject to HIPAA to use the secure AWS environment to process, maintain, and store protected health information. For instructions on how you can use AWS for the processing and storage of health information, see the [Architecting for HIPAA Security and Compliance on Amazon Web Services](#) whitepaper.

Using this framework to support your audit preparation

You can use the *HIPAA Final Omnibus Security Rule 2013* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These

controls are grouped into control sets according to HIPAA requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the HIPAA framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The HIPAA Final Omnibus Security Rule 2013 framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
HIPAA Final Omnibus Security Rule 2013	39	46	5	<ul style="list-style-type: none">Amazon Elastic Compute CloudAWS CloudTrailAWS ConfigAWS Identity and Access ManagementAWS Security Hub

Tip

To review the AWS Config rules that are used as data source mappings in this standard framework, download the [AuditManager_ConfigDataSourceMappings_HIPAA-Final-Omnibus-Security-Rule-2013.zip](#) file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with the HIPAA standard. Moreover, they can't guarantee that you'll pass a HIPAA audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find this framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the HIPAA framework. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More HIPAA resources

- [Health Information Privacy](#) from the U.S. Department of Health and Human Service
- [Omnibus HIPAA Rulemaking](#) from the U.S. Department of Health and Human Service
- [Architecting for HIPAA Security and Compliance on Amazon Web Services](#)

- [AWS Compliance page for HIPAA](#)

ISO/IEC 27001:2013 Annex A

AWS Audit Manager provides a prebuilt standard framework that structures and automates assessments for ISO/IEC 27001:2013 Annex A.

Topics

- [What is ISO/IEC 27001:2013 Annex A? \(p. 189\)](#)
- [Using this framework to support your audit preparation \(p. 189\)](#)
- [More ISO/IEC 27001:2013 Annex A resources \(p. 190\)](#)

What is ISO/IEC 27001:2013 Annex A?

The International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO) are both independent, non-governmental, not-for-profit organizations that develop and publish fully consensus-based international standards.

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/IEC 27002 best practice guidance. This international standard specifies the requirements on how to establish, implement, maintain, and continually improve an information security management system at your organization. Included among these standards are requirements on the assessment and treatment of information security risks that are tailored to the needs of your organization. The requirements in this international standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

Using this framework to support your audit preparation

You can use the AWS Audit Manager framework for ISO/IEC 27001:2013 Annex A to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to ISO/IEC 27001:2013 Annex A requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for an ISO/IEC 27001:2013 Annex A audit. In your assessment, you can specify the AWS accounts and services that you want to include in the scope of your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the ISO/IEC 27001:2013 Annex A framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
ISO-IEC 27001:2013 Annex A	50	64	35	<ul style="list-style-type: none">• Amazon CloudWatch• Amazon Elastic Compute Cloud• AWS CloudTrail

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
				<ul style="list-style-type: none">• AWS Config• AWS Identity and Access Management• AWS Security Hub

Tip

To review the AWS Config rules that are used as data source mappings in this standard framework, download the [AuditManager_ConfigDataSourceMappings_ISO-IEC-27001-2013-Annex-A.zip](#) file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with this international standard. Moreover, they can't guarantee that you'll pass an ISO/IEC audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find the ISO/IEC 27001:2013 Annex A framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the ISO-IEC 27001:2013 Annex A framework. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#). For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More ISO/IEC 27001:2013 Annex A resources

- For more information about this international standard, see [ISO/IEC 27001:2013](#) on the ANSI Webstore.

NIST 800-53 (Rev. 5) Low-Moderate-High

AWS Audit Manager provides a prebuilt framework that structures and automates assessments for the NIST 800-53 compliance standard, based on AWS best practices.

Note

- For information about the Audit Manager framework that supports *NIST 800-171*, see [NIST SP 800-171 \(Rev. 2\) \(p. 194\)](#).
- For information about the Audit Manager framework that supports the *NIST Cybersecurity Framework*, see [NIST Cybersecurity Framework version 1.1 \(p. 192\)](#).

Topics

- [What is NIST 800-53? \(p. 191\)](#)

- [Using this framework to support your audit preparation \(p. 191\)](#)
- [More NIST resources \(p. 192\)](#)

What is NIST 800-53?

The [National Institute of Standards and Technology \(NIST\)](#) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the oldest physical science laboratories in the United States. The U.S. Congress established the agency to improve what was at the time a second-rate measurement infrastructure. The infrastructure was a major challenge to U.S. industrial competitiveness, having lagged behind other economic powers such as the U.K. and Germany.

The NIST 800-53 security controls are generally applicable to U.S. federal information systems. These are typically systems that must go through a formal assessment and authorization process. This process ensures sufficient protection of confidentiality, integrity, and availability of information and information systems. This is based on the security category and impact level of the system (low, moderate, or high) as well as a risk determination. Security controls are selected from the NIST SP 800-53 security control catalog, and the system is assessed against those security control requirements.

The NIST 800-53 (Rev. 5) Low-Moderate-High framework represents the security controls and the associated assessment procedures that are defined in NIST SP 800-53 Revision 5 Recommended Security Controls for Federal Information Systems and Organizations. For any discrepancies that are noted in the content between this NIST SP 800-53 framework and the latest published NIST Special Publication SP 800-53 Revision 5, refer to the official published documents that are available at the [NIST Computer Security Resource Center](#).

Using this framework to support your audit preparation

You can use the *NIST 800-53 (Rev. 5) Low-Moderate-High* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to NIST requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the NIST 800-53 (Rev. 5) Low-Moderate-High framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The NIST 800-53 (Rev. 5) Low-Moderate-High framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
NIST 800-53 (Rev. 5) Low-Moderate-High	225	782	280	<ul style="list-style-type: none">• Amazon CloudWatch• Amazon Elastic Compute Cloud• AWS CloudTrail• AWS Config• AWS Identity and Access Management• AWS Security Hub

Tip

To review the AWS Config rules that are used as data source mappings in this standard framework, download the [AuditManager_ConfigDataSourceMappings_NIST-800-53-Rev.5-Low-Moderate-High.zip](#) file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with the NIST standard. Moreover, they can't guarantee that you'll pass a NIST audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find this framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the NIST 800-53 (Rev. 5) Low-Moderate-High framework. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More NIST resources

- [National Institute of Standards and Technology \(NIST\)](#)
- [NIST Computer Security Resource Center](#)
- [AWS Compliance page for NIST](#)

NIST Cybersecurity Framework version 1.1

AWS Audit Manager provides a prebuilt framework that structures and automates assessments for the NIST Cybersecurity Framework, based on AWS best practices.

Note

- For information about the Audit Manager framework that supports *NIST 800-53 (Rev. 5) Low-Moderate-High*, see [NIST 800-53 \(Rev. 5\) Low-Moderate-High \(p. 190\)](#).
- For information about the Audit Manager framework that supports *NIST SP 800-171 (Rev. 2)*, see [NIST SP 800-171 \(Rev. 2\) \(p. 194\)](#).

Topics

- [What is the NIST Cybersecurity Framework? \(p. 192\)](#)
- [Using this framework to support your audit preparation \(p. 193\)](#)
- [More NIST resources \(p. 194\)](#)

What is the NIST Cybersecurity Framework?

The [National Institute of Standards and Technology \(NIST\)](#) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the oldest physical science laboratories in the United States. The U.S. Congress established the agency to improve what was at the time a second-rate

measurement infrastructure. The infrastructure was a major challenge to U.S. industrial competitiveness, having lagged behind other economic powers like the U.K. and Germany.

The United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and interconnectedness of critical infrastructure systems. They put the security, economy, and public safety and health of the United States at risk. Similar to financial and reputational risks, cybersecurity risk affects a company's bottom line. It can drive up costs and affect revenue. It can harm an organization's ability to innovate and to gain and maintain customers. Ultimately, cybersecurity can amplify the overall risk management of an organization.

The NIST Cybersecurity Framework (CSF) is supported by governments and industries worldwide as a recommended baseline for use by any organization, regardless of sector or size. The NIST Cybersecurity Framework consists of three primary components: the framework core, the profiles, and the implementation tiers. The framework core contains desired cybersecurity activities and outcomes organized into 23 categories that cover the breadth of cybersecurity objectives for an organization. The profiles contain an organization's unique alignment of their organizational requirements and objectives, risk appetite, and resources using the desired outcomes of the framework core. The implementation tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the framework core.

Using this framework to support your audit preparation

You can use the *NIST Cybersecurity Framework version 1.1* to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to NIST CSF requirements. Audit Manager currently supports the framework core component by offering 56 automated controls and 52 manual controls. These controls are matched to 23 cybersecurity categories that are defined in the framework core. Audit Manager doesn't support the profile and implementation components in this framework.

You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the NIST Cybersecurity Framework version 1.1. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The details for NIST Cybersecurity Framework version 1.1 are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
NIST Cybersecurity Framework version 1.1	56	52	23	<ul style="list-style-type: none">• AWS Config• AWS Identity and Access Management• AWS Security Hub

Tip

To review the AWS Config rules that are used as data source mappings in this standard framework, download the [AuditManager_ConfigDataSourceMappings_NIST-CSF-v1.1.zip](#) file.

The controls that are offered by Audit Manager aren't intended to verify if your systems are compliant with the NIST Cybersecurity Framework. Moreover, they can't guarantee that you'll pass a NIST

Cybersecurity audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find this framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the NIST Cybersecurity Framework version 1.1 framework. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More NIST resources

- [National Institute of Standards and Technology \(NIST\)](#)
- [NIST Computer Security Resource Center](#)
- [AWS Compliance page for NIST](#)
- [NIST Cybersecurity Framework - Aligning to the NIST CSF in the AWS Cloud](#)

NIST SP 800-171 (Rev. 2)

AWS Audit Manager provides a prebuilt framework that structures and automates assessments for the NIST SP 800-171 compliance standard based on AWS best practices.

Note

- For information about the Audit Manager framework that supports *NIST 800-53 (Rev. 5) Low-Moderate-High*, see [NIST 800-53 \(Rev. 5\) Low-Moderate-High \(p. 190\)](#).
- For information about the Audit Manager framework that supports *NIST Cybersecurity Framework version 1.1*, see [NIST Cybersecurity Framework version 1.1 \(p. 192\)](#).

Topics

- [What is NIST SP 800-171? \(p. 194\)](#)
- [Using this framework to support your audit preparation \(p. 195\)](#)
- [More NIST resources \(p. 196\)](#)

What is NIST SP 800-171?

NIST SP 800-171 focuses on protecting the confidentiality of Controlled Unclassified Information (CUI) in nonfederal systems and organizations. It recommends specific security requirements to achieve that objective. NIST 800-171 is a publication that outlines the required security standards and practices for nonfederal organizations that handle CUI on their networks. It was first published in June 2015 by the [National Institute of Standards and Technology \(NIST\)](#). NIST is a U.S. government agency that released several standards and publications to strengthen cybersecurity resilience in the public and private sectors. NIST 800-171 has received regular updates in line with emerging cyber threats and changing technologies. The latest version (revision 2) was released in February 2020.

The cybersecurity controls within NIST 800-171 safeguard CUI in the IT networks of government contractors and subcontractors. It defines the practices and procedures that government contractors must adhere to when their networks process or store CUI. NIST 800-171 only applies to those parts of a contractor's network where CUI is present.

Using this framework to support your audit preparation

You can use the *NIST SP 800-171 Rev. 2* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to NIST requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the NIST SP 800-171 Rev. 2 framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The NIST SP 800-171 Rev. 2 framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
NIST SP 800-171 Rev. 2	66	58	16	<ul style="list-style-type: none">Amazon CloudWatchAmazon Elastic Compute CloudAWS CloudTrailAWS ConfigAWS Identity and Access ManagementAWS Security Hub

Tip

To review the AWS Config rules that are used as data source mappings in this standard framework, download the [AuditManager_ConfigDataSourceMappings_NIST-SP-800-171-Rev.2.zip](#) file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with NIST 800-171. Moreover, they can't guarantee that you'll pass a NIST audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find this framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For information about how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the NIST SP 800-171 Rev. 2 framework. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API

operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More NIST resources

- [National Institute of Standards and Technology \(NIST\)](#)
- [NIST Computer Security Resource Center](#)
- [AWS Compliance page for NIST](#)

PCI DSS V3.2.1

AWS Audit Manager provides a prebuilt framework that supports PCI DSS v3.2.1.

Topics

- [What is PCI DSS? \(p. 196\)](#)
- [Using this framework to support your audit preparation \(p. 196\)](#)
- [More PCI DSS resources \(p. 197\)](#)

What is PCI DSS?

The *Payment Card Industry Data Security Standard (PCI DSS)* is a proprietary information security standard. It's administered by the [PCI Security Standards Council](#), which was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. PCI DSS applies to entities that store, process, or transmit cardholder data (CHD) or sensitive authentication data (SAD). This includes, but isn't limited to, merchants, processors, acquirers, issuers, and service providers. The PCI DSS is mandated by the card brands and administered by the Payment Card Industry Security Standards Council.

AWS is certified as a PCI DSS Level 1 Service Provider, which is the highest level of assessment available. The compliance assessment was conducted by Coalfire Systems Inc., an independent Qualified Security Assessor (QSA). The PCI DSS Attestation of Compliance (AOC) and Responsibility Summary are available to you through AWS Artifact. This is a self-service portal for on-demand access to AWS compliance reports. Sign in to [AWS Artifact in the AWS Management Console](#), or learn more at [Getting Started with AWS Artifact](#).

You can download the PCI DSS standard from the [PCI Security Standards Council Document Library](#).

Using this framework to support your audit preparation

You can use the *PCI DSS V3.2.1* framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to PCI DSS requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the PCI DSS V3.2.1 framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The PCI DSS V3.2.1 framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
PCI DSS V3.2.1	175	487	12	<ul style="list-style-type: none">Amazon Elastic Compute CloudAWS CloudTrailAWS ConfigAWS Identity and Access ManagementAWS Security Hub

Tip

To review the AWS Config rules that are used as data source mappings in this standard framework, download the [AuditManager_ConfigDataSourceMappings_PCI-DSS-V3.2.1.zip](#) file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant with the PCI DSS standard. Moreover, they can't guarantee that you'll pass a PCI DSS audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find this framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For information about how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the PCI DSS V3.2.1 framework. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More PCI DSS resources

- [PCI Security Standards Council](#)
- [PCI Security Standards Council Document Library](#).
- [AWS Compliance page for PCI DSS](#)

SOC 2

SOC 2 is an auditing procedure that ensures a company's data is securely managed. AWS Audit Manager provides a prebuilt framework that supports SOC 2.

Topics

- [What is SOC 2? \(p. 198\)](#)
- [Using this framework to support your audit preparation \(p. 198\)](#)

- [More SOC 2 resources \(p. 199\)](#)

What is SOC 2?

System and Organization Controls (SOC), defined by the [American Institute of Certified Public Accountants](#) (AICPA), is the name of a set of reports that's produced during an audit. It's intended for use by service organizations (organizations that provide information systems as a service to other organizations) to issue validated reports of [internal controls](#) over those information systems to the users of those services. The reports focus on controls grouped into five categories known as *Trust Service Principles*.

AWS SOC reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help you and your auditors understand the AWS controls established to support operations and compliance. There are five AWS SOC reports:

- AWS SOC 1 Report, available to AWS customers from [AWS Artifact](#).
- AWS SOC 2 Security, Availability & Confidentiality Report, available to AWS customers from [AWS Artifact](#).
- AWS SOC 2 Security, Availability & Confidentiality Report available to AWS customers from [AWS Artifact](#) (scope includes Amazon DocumentDB only).
- AWS SOC 2 Privacy Type I Report, available to AWS customers from [AWS Artifact](#).
- AWS SOC 3 Security, Availability & Confidentiality Report, [publicly available as a whitepaper](#).

Using this framework to support your audit preparation

You can use this framework to help you prepare for audits. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped into control sets according to SOC 2 requirements. You can also customize this framework and its controls to support internal audits with specific requirements.

Using the framework as a starting point, you can create an Audit Manager assessment and start collecting evidence that's relevant for your audit. After you create an assessment, Audit Manager starts to assess your AWS resources. It does this based on the controls that are defined in the framework. When it's time for an audit, you—or a delegate of your choice—can review the collected evidence and then add it to an assessment report. You can use this assessment report to show that your controls are working as intended.

The framework details are as follows:

Framework name in AWS Audit Manager	Number of automated controls	Number of manual controls	Number of control sets	AWS services in scope
SOC 2	20	41	20	<ul style="list-style-type: none">• Amazon Elastic Compute Cloud• AWS Auto Scaling• AWS CloudTrail• AWS Config• AWS Identity and Access Management• AWS Security Hub

Tip

To review the AWS Config rules that are used as data source mappings in this standard framework, download the [AuditManager_ConfigDataSourceMappings_SOC2.zip](#) file.

The controls in this AWS Audit Manager framework aren't intended to verify if your systems are compliant. Moreover, they can't guarantee that you'll pass an audit. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find this framework under the **Standard frameworks** tab of the [Framework library \(p. 107\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 50\)](#).

When you use the Audit Manager console to create an assessment from this standard framework, the list of AWS services in scope is selected by default and can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to SOC 2 requirements. If you need to edit the list of services in scope for this framework, you can do so by using the [CreateAssessment](#) or [UpdateAssessment](#) API operations. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

More SOC 2 resources

- [AWS Compliance page for SOC](#)

Control library

You can access and manage controls from the *control library* in Audit Manager. You can go to the control library at any time by choosing **Control library** in the navigation pane in the Audit Manager console.

The control library contains a catalog of standard controls and custom controls.

- **Standard controls** are predefined controls that are provided by AWS. You can view the configuration details of standard controls, but you can't edit or delete them. However, you can customize any standard control to create a new one that meets your specific requirements.
- **Custom controls** are customized controls that you own and define. With a custom control, you can specify which data sources you want to collect evidence from. You can then add custom controls to a custom framework.

To learn more about how to add a custom control to a custom framework, see [Framework library \(p. 107\)](#). To learn more about how to create an assessment from an Audit Manager framework, see [Assessments in AWS Audit Manager \(p. 50\)](#).

This section describes how you can create and manage custom controls in Audit Manager.

Topics

- [Accessing the available controls in AWS Audit Manager \(p. 200\)](#)
- [Reviewing the details of a control \(p. 201\)](#)
- [Creating a custom control \(p. 203\)](#)
- [Editing a custom control \(p. 208\)](#)
- [Deleting a custom control \(p. 210\)](#)
- [Changing the evidence collection frequency for a control \(p. 211\)](#)
- [Supported control data sources for automated evidence \(p. 213\)](#)

Accessing the available controls in AWS Audit Manager

You can view all available controls on the **Control library** page in the Audit Manager console. From here, you can also [create a custom control](#) or [customize an existing control](#).

You can also view all available controls using the Audit Manager API or the AWS Command Line Interface (AWS CLI).

Audit Manager console

To view available controls (console)

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Control library**.
3. Choose the **Standard controls** tab or the **Custom controls** tab to browse the available controls.
4. Choose any control name to view the details for that control.

AWS CLI

To view available controls (AWS CLI)

Run the [list-controls](#) command and specify a --control-type. Either, you can retrieve a list of standard controls. Or, you can retrieve a list of custom controls.

```
aws auditmanager list-controls --control-type Standard
```

```
aws auditmanager list-controls --control-type Custom
```

Audit Manager API

To view available controls (API)

Use the [ListControls](#) operation and specify a [controlType](#). Either, you can return a list of standard controls. Or, you can return a list of custom controls.

For more information, choose either of the previous links to read more in the *AWS Audit Manager API Reference*. This includes information about how to use the ListControls operation and parameters in one of the language-specific AWS SDKs.

Reviewing the details of a control

You can review the details of a control using the Audit Manager console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI).

Audit Manager console

To view control details (console)

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Control library** to see a list of available controls.
3. Choose the **Standard controls** tab or the **Custom controls** tab to browse the available controls.
4. Choose any control name to view the details for that control.

When you open a control, you see a control details page. The sections of this page and their contents are described below.

Summary section

This section provides an overview of the control. It includes the following information:

- **Control name** – The name of the control.
- **Control type** – Specifies whether the control is a standard control or a custom control.
- **Tags** – The number of tags that are associated with the control.
- **Data source types** – The number of [data source types](#) that are used for this control.
- **Mappings** – The number of [mapping](#) attributes that are used to retrieve data from a data source.

If you're viewing a custom control, the following details are also displayed:

- **Created by** – The account that created the custom control.
- **Creation date** – The date when the custom control was created.

- **Last updated** – The date when the custom control was last edited.

Details tab

This tab provides a basic overview of the control. It includes the following information:

- The **Description** section provides a description of the control.
- The **Testing information** section provides a description of the recommended testing procedures for the control.
- The **Action plan** section describes the recommended actions to carry out if the control needs to be remediated.

Data sources tab

This tab displays information about the data sources for the control. It includes the following information:

- **Data source name** – This applies to custom controls only. It refers to the descriptive name that you gave each data source. You can use this name to distinguish between multiple data sources that fall under the same data source type.
- **Data source type** – This specifies where the evidence data comes from.
 - If Audit Manager collects the evidence, the data source can be one of four types: *AWS Security Hub*, *AWS Config*, *AWS CloudTrail*, or *AWS API calls*.
 - If you upload your own evidence, the data source type is *Manual*. A description indicates if the required manual evidence is a *File upload* or a *Text response*.
- **Mapping** – This is the mapping attribute that's used to identify and retrieve data from the data source.
 - If the data source type is AWS Config, the mapping is the name of a specific AWS Config rule (for example, EC2_INSTANCE_MANAGED_BY_SSM). Audit Manager uses this mapping to report the result of that rule check directly from AWS Config.
 - If the data source type is AWS Security Hub, the mapping is the name of a specific Security Hub control (for example, 1.1 – Avoid the use of the "root" account). Audit Manager uses this mapping to report the result of that security check directly from Security Hub.
 - If the data source type is AWS API calls, the mapping is the name of a specific API call (for example, ec2_DescribeSecurityGroups). Audit Manager uses this mapping to collect the API response.
 - If the data source is AWS CloudTrail, the mapping is the name of a specific CloudTrail event (for example, CreateAccessKey). Audit Manager uses this mapping to collect the related user activity from your CloudTrail logs.
- **Frequency** – This specifies how often Audit Manager collects evidence from the data source. The frequency varies depending on the data source type. For more information, choose the value in the column or see [Evidence collection frequency \(p. 12\)](#).

Tags tab

This tab lists the tags that are associated with the control. It includes the following information:

- **Key** – The tag key (for example, a compliance standard, regulation, or category).
- **Value** – The tag value.

AWS CLI

To view control details (AWS CLI)

1. To identify the control that you want to review, run the [list-controls](#) command and specify a --control-type. Either, you can retrieve a list of standard controls. Or, you can retrieve a list of custom controls.

In the following example, replace the *placeholder text* with either Custom or Standard.

```
aws auditmanager list-controls --control-type Custom/Standard
```

The response returns a list of controls. Find the control that you want to review, and take note of the control ID and Amazon Resource Name (ARN).

2. To get the control details, run the [get-control](#) command and specify the --control-id.

In the following example, replace the *placeholder text* with your own information.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

The control details are returned in JSON format. To understand this data, see [get-control Output](#) in the *AWS CLI Command Reference*.

3. To see the tags for a control, use the [list-tags-for-resource](#) command and specify the --resource-arn for the control.

In the following example, replace the *placeholder text* with your own information:

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

For more information about tags in Audit Manager, see [Tagging AWS Audit Manager resources](#).

Audit Manager API

To view control details (API)

1. To identify the control that you want to review, use the [ListControls](#) operation and specify a [controlType](#). Either, you can return a list of standard controls. Or, you can return a list of custom controls.

From the response, find the control that you want to review, and take note of the control ID and its Amazon Resource Name (ARN).

2. To get the control details, use the [GetControl](#) operation. In the request, specify the [controlId](#) that you got from step 1.

The control details are returned in JSON format. To understand this data, see [GetControl Response Elements](#) in the *AWS Audit Manager API Reference*.

3. To see tags for the control, use the [ListTagsForResource](#) operation. In the request, specify the control [resourceArn](#) that you got from step 1.

For more information about tags in Audit Manager, see [Tagging AWS Audit Manager resources](#).

For more information about these API operations, choose any of the previous links to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Creating a custom control

You can use custom controls to collect evidence from specific data sources that you define.

Just like standard controls, custom controls collect evidence continually when they're active in your assessments. You can also add manual evidence to any custom control that you create. Each piece of evidence becomes a record that helps you to demonstrate compliance with your custom control's requirements.

To get started, here are some examples of how you can use custom controls:

Use an existing control as a starting point

You can customize any control in Audit Manager. This is a good option if an existing control more or less meets your objective, but you want to extend its guidance or adjust a few attributes to meet your specific needs. For example, you might change how often a control collects evidence, and then change the control's name to reflect this.

Create a custom control for internal audits

To support internal audits, you can create a purpose-built custom control that's not related to any specific compliance framework or regulation. This gives you the freedom to tailor your control's requirements to a particular area, or collect evidence from a business-specific resource. For example, you can create a custom control that uses your organization's custom AWS Config rules as a data source for evidence collection.

Create a vendor risk assessment question

You can use custom controls to support how you manage vendor risk assessments. Each control that you create can represent an individual risk assessment question. In this case, the control name can be a question, and you can provide an answer by uploading a file or entering a text response as manual evidence.

There are two ways to create a custom control. You can create a new control from scratch or you can customize an existing control.

Topics

- [Creating a new custom control from scratch \(p. 204\)](#)
- [Customizing an existing control \(p. 206\)](#)

Creating a new custom control from scratch

You can create a new custom control from scratch by following these steps.

Important

We strongly recommend that you never put sensitive identifying information into free-form fields such as **Control details**, **Testing information**, or **Action plan**. If you create custom controls that contain sensitive information, you can't share any of your custom frameworks that contain these controls.

Topics

- [Step 1: Specify control details \(p. 204\)](#)
- [Step 2: Set up data sources \(p. 205\)](#)
- [Step 3 \(Optional\): Define an action plan \(p. 206\)](#)
- [Step 4: Review and create the control \(p. 206\)](#)
- [What can I do next? \(p. 206\)](#)

Step 1: Specify control details

Start by specifying the details of your custom control.

To specify control details

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Control library**, and then choose **Create custom control**.
3. Under **Control details**, enter the following information about the control.
 - **Control** – Enter a friendly name, a title, or a risk assessment question. This value helps you to identify your control in the control library.
 - **Description (optional)** – Enter details to help others understand the control's objective. This description appears on the control details page.
4. Under **Testing information**, enter the recommended steps for testing the control.
5. Under **Tags**, choose **Add new tag** to associate a tag with the control. You can specify a key for each tag that best describes the compliance framework that this control supports. The tag key is mandatory and can be used as a search criteria when you search for this control in the control library.
6. Choose **Next**.

Step 2: Set up data sources

Next, define up to 10 data sources. A data source determines where your custom control collects evidence from.

If you want to collect automated evidence, each data source must include a data source type and a data source mapping. These details map to your AWS usage, and tell Audit Manager where to collect the evidence from. If you want to provide your own evidence instead, you'll name your data source and then choose a manual evidence option.

Important

To successfully use AWS Config and Security Hub as automated data sources, make sure that you do the following:

- Follow the instructions to [set up AWS Config](#) and [set up Security Hub](#) for use with Audit Manager.
- Include both AWS Config and Security Hub as services in scope in your assessment.

Audit Manager can then collect evidence each time an evaluation occurs for the AWS Config rules or the Security Hub controls that you specify in this step.

To set up data sources

1. Under **Data source name**, replace the placeholder text with a descriptive name for the data source.
2. Under **Evidence collection method**, choose how you want to collect evidence for this control.
 - a. If you want Audit Manager to collect evidence, choose **Automated** and follow these steps:
 - Under **Data source type**, specify where Audit Manager collects automated evidence from.
 - For **AWS CloudTrail**, choose an event name keyword from the dropdown list.
 - For **AWS Config**, select a rule type and then choose a rule identifier keyword from the dropdown list.
 - For **AWS Security Hub**, choose a Security Hub control from the dropdown list.
 - For **AWS API calls**, choose an API call and then select an evidence collection frequency.

Tip

For an overview of each data source type and related troubleshooting tips, see [Overview of automated data sources \(p. 214\)](#).

If you need to validate your data source configuration with a domain expert, set the evidence collection method as **Manual** for now. That way, you can create the control and add it to a framework now, and then [edit the control](#) as needed later.

- b. If you want to provide your own evidence, choose **Manual** and select a **Manual evidence option**.
 - **File upload** – Select this option if the control requires documentation as evidence.
 - **Text response** – Select this option if the control requires an answer to a risk assessment question.
3. (Optional) Under **Additional details**, enter a data source description and a troubleshooting description.
4. (Optional) To add another data source, choose **Add data source** and repeat steps 1-3.
5. (Optional) To remove a data source, choose **Remove** at the top of the data source configuration box.
6. When you're finished, choose **Next**.

Step 3 (Optional): Define an action plan

Next, specify the actions to take if this control needs to be remediated.

To define an action plan

1. Under **Title**, enter a descriptive title for the action plan.
2. Under **Action plan instructions**, enter detailed instructions for the action plan.
3. Choose **Next**.

Step 4: Review and create the control

Review the information for the control. To change the information for a step, choose **Edit**.

When you're finished, choose **Create custom control**.

What can I do next?

After you create a new custom control, you can add it to a custom framework. To learn more, see [Creating a custom framework \(p. 110\)](#) or [Editing a custom framework \(p. 114\)](#).

After you add the custom control to a custom framework, you can create an assessment from that custom framework and start collecting evidence. To learn more, see [Creating an assessment \(p. 50\)](#).

For troubleshooting tips, see [Troubleshooting control and control set issues \(p. 282\)](#).

Customizing an existing control

Instead of creating a custom control from scratch, you can use an existing control as a starting point and customize it according to your needs. When you do this, the existing control remains in the control library, and a new custom control is created with your customized settings.

You can select any existing control to customize. It can be either a standard control or a custom control.

Important

We strongly recommend that you never put sensitive identifying information into free-form fields such as **Control details**, **Testing information**, or **Action plan**. If you create custom controls that contain sensitive information, you can't share any of your custom frameworks that contain these controls.

Topics

- [Step 1: Specify control details \(p. 207\)](#)
- [Step 2: Set up data sources \(p. 207\)](#)
- [Step 3: \(Optional\): Define an action plan \(p. 208\)](#)
- [Step 4: Review and create the control \(p. 208\)](#)
- [What can I do next? \(p. 208\)](#)

Step 1: Specify control details

The control details are inherited from the original control. Review and modify these details as needed.

To specify control details

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Control library**.
3. Select the control that you want to customize and then choose **Customize existing control**.
4. Specify the new name of the control, and choose **Customize**.
5. Under **Control details**, customize the control details as needed.
6. Under **Testing information**, customize the testing information as needed.
7. Under **Tags**, customize the tags as needed.
8. Choose **Next**.

Step 2: Set up data sources

Data sources are inherited from the original control. You can change, add, or remove data sources as needed.

Important

To successfully use AWS Config and Security Hub as automated data sources, make sure that you do the following:

- Follow the instructions to [set up AWS Config](#) and [set up Security Hub](#) for use with Audit Manager.
- Include both AWS Config and Security Hub as services in scope in your assessment.

Audit Manager can then collect evidence each time an evaluation occurs for the AWS Config rules or the Security Hub controls that you specify in this step.

To set up data sources

1. Under **Data source name**, customize the data source name as needed.
2. Under **Evidence collection method**, customize the selection as needed.
 - a. If you want Audit Manager to collect evidence, choose **Automated** and follow these steps:
 - Under **Data source type**, review where Audit Manager collects automated evidence from, and modify as needed.
 - For **AWS CloudTrail**, choose an event name keyword from the dropdown list.
 - For **AWS Config**, select a rule type and then choose a rule identifier keyword from the dropdown list.

- For **AWS Security Hub**, choose a Security Hub control from the dropdown list.
- For **AWS API calls**, choose an API call and then select an evidence collection frequency.

Tip

For an overview of each data source type and related troubleshooting tips, see [Overview of automated data sources \(p. 214\)](#).

If you need to validate your data source configuration with a domain expert, set the evidence collection method as **Manual** for now. That way, you can create the control and add it to a framework now, and then [edit the control](#) as needed later.

- b. If you want to provide your own evidence, choose **Manual** and select a **Manual evidence option**.
 - **File upload** – Select this option if the control requires documentation as evidence.
 - **Text response** – Select this option if the control requires an answer to a risk assessment question.
3. (Optional) Under **Additional details**, make any necessary changes to the data source description or the troubleshooting description.
4. (Optional) To add another data source, choose **Add data source**.
5. (Optional) To remove a data source, choose **Remove**.
6. Choose **Next**.

Step 3: (Optional): Define an action plan

The action plan is inherited from the original control. You can edit this action plan as needed.

To define an action plan

1. Under **Title**, review the title for the action plan, and customize it as needed.
2. Under **Action plan instructions**, review and customize the instructions as needed.
3. Choose **Next**.

Step 4: Review and create the control

Review the information for the control. To change the information for a step, choose **Edit**. When you're finished, choose **Create custom control**.

What can I do next?

After you create a new custom control, you can add it to a custom framework. To learn more, see [Creating a custom framework \(p. 110\)](#) or [Editing a custom framework \(p. 114\)](#).

After you add a custom control to a custom framework, you can create an assessment from that custom framework and start collecting evidence. To learn more, see [Creating an assessment \(p. 50\)](#).

If you need to edit a custom control, see [Editing a custom control \(p. 208\)](#).

For troubleshooting tips, see [Troubleshooting control and control set issues \(p. 282\)](#).

Editing a custom control

You can edit a custom control in Audit Manager by following these steps.

Topics

- [Step 1: Edit control details \(p. 209\)](#)
- [Step 2: Edit data sources \(p. 209\)](#)
- [Step 3: \(Optional\) Edit an action plan \(p. 210\)](#)
- [Step 4: Review and update the control \(p. 210\)](#)

Step 1: Edit control details

Start by reviewing and editing the control details as needed.

To edit control details

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Control library** and then choose the **Custom controls** tab.
3. Select the control that you want to edit and then choose **Edit**.
4. Under **Control details**, edit the control details as needed.
5. Under **Testing information**, edit the recommended testing information as needed.
6. Choose **Next**.

Tip

To edit the tags for a control, open the control and choose the [tags tab](#). There you can view and edit the tags that are associated with the control.

Step 2: Edit data sources

Next, you can edit, remove, or add data sources for the control.

Important

To successfully use AWS Config and Security Hub as automated data sources, make sure that you do the following:

- Follow the instructions to [set up AWS Config](#) and [set up Security Hub](#) for use with Audit Manager.
- Include both AWS Config and Security Hub as services in scope in your assessment.

Audit Manager can then collect evidence each time an evaluation occurs for the AWS Config rules or the Security Hub controls that you specify in this step.

To edit data sources

1. Under **Data source name**, review the current name and edit it as needed.
2. Under **Evidence collection method**, review the current selection and edit as needed.
 - a. If you want Audit Manager to collect evidence, choose **Automated** and follow these steps:
 - Under **Data source type**, review where Audit Manager collects automated evidence from, and edit as needed.
 - For **AWS CloudTrail**, choose an event name keyword from the dropdown list.
 - For **AWS Config**, select a rule type and then choose a rule identifier keyword from the dropdown list.
 - For **AWS Security Hub**, choose a Security Hub control from the dropdown list.

- For **AWS API calls**, choose an API call and then select an evidence collection frequency.

Tip

For an overview of each data source type and related troubleshooting tips, see [Overview of automated data sources \(p. 214\)](#).

- b. If you want to provide your own evidence, choose **Manual** and select a **Manual evidence option**.
 - **File upload** – Select this option if the control requires documentation as evidence.
 - **Text response** – Select this option if the control requires an answer to a risk assessment question.
3. (Optional) Under **Additional details**, make any necessary changes to the data source description or the troubleshooting description.
4. (Optional) To add another data source, choose **Add data source**.
5. (Optional) To remove a data source, choose **Remove**.
6. Choose **Next**.

Step 3: (Optional) Edit an action plan

Next, review and edit the optional action plan.

To edit an action plan

1. Under **Title**, edit the title as needed.
2. Under **Action plan instructions**, edit the instructions as needed.
3. Choose **Next**.

Step 4: Review and update the control

Review the information for the control. To change the information for a step, choose **Edit**.

When you're finished, choose **Save changes**.

Note

After you edit a control, the changes take effect as follows in all active assessments that include the control:

- For controls with *AWS API calls* as the data source type, changes take effect at 00:00 UTC the following day.
- For all other controls, changes take effect immediately.

Deleting a custom control

You can use the control library to delete an unwanted custom control. After you delete a control, it no longer appears in the control library. You can also delete custom controls using the Audit Manager API or the AWS Command Line Interface (AWS CLI).

Important

When you delete a custom control, this action removes the control from any custom frameworks or assessments that it's currently related to. As a result, Audit Manager will stop collecting evidence for that custom control in all of your assessments. This includes assessments that you previously created before you deleted the custom control.

Audit Manager console

To delete a custom control (console)

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Control library** and then choose the **Custom controls** tab.
3. Select the control that you want to delete, and then choose **Delete**.
4. In the pop-up window that appears, choose **Delete** to confirm deletion.

AWS CLI

To delete a custom control (AWS CLI)

1. First, identify the custom control that you want to delete. To do this, run the [list-controls](#) command and specify the --control-type as Custom.

```
aws auditmanager list-controls --control-type Custom
```

The response returns a list of custom controls. Find the control that you want to delete, and take note of the control ID.

2. Next, run the [delete-control](#) command and use the --control-id parameter to specify the control that you want to delete.

In the following example, replace the *placeholder text* with your own information.

```
aws auditmanager delete-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

To delete a custom control (API)

1. Use the [ListControls](#) operation and specify the `controlType` as Custom. From the response, find the control that you want to delete and note the control ID.
2. Use the [DeleteControl](#) operation to delete the custom control. In the request, use the `controlId` parameter to specify the control that you want to delete.

For more information about these API operations, choose any of the previous links to read more in the *AWS Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

Changing the evidence collection frequency for a control

AWS Audit Manager collects evidence from multiple data sources at varying frequencies. The supported evidence collection frequency depends on the type of evidence that is collected for the control.

- For **AWS API calls**, Audit Manager collects evidence using a describe API call to another AWS service. You can specify the evidence collection frequency directly in Audit Manager (for custom controls only).
- For **AWS Config**, Audit Manager reports the result of a compliance check directly from AWS Config. The frequency follows the triggers that are defined in the AWS Config rule.

- For **AWS Security Hub**, Audit Manager reports the result of a compliance check directly from Security Hub. The frequency follows the schedule of the Security Hub check.
- For **AWS CloudTrail**, Audit Manager collects evidence continuously from CloudTrail. You can't change the frequency for this evidence type.

The following sections provide more information about the evidence collection frequency for each control data source type, and how to change it (if applicable).

Topics

- [Configuration snapshots from AWS API calls \(p. 212\)](#)
- [Compliance checks from AWS Config \(p. 212\)](#)
- [Compliance checks from Security Hub \(p. 213\)](#)
- [User activity logs from AWS CloudTrail \(p. 213\)](#)

Configuration snapshots from AWS API calls

Note

The following applies only to custom controls. You can't change the evidence collection frequency for a standard control that uses API calls as a data source.

If a custom control uses AWS API calls as a data source type, you can change the evidence collection frequency in Audit Manager by following these steps.

To change the evidence collection frequency for a custom control with an API call data source

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the navigation pane, choose **Control library**, and then choose the **Custom controls** tab.
3. Choose the custom control that you want to edit, and then choose **Edit**.
4. On the **Edit control details** page, choose **Next**.
5. Find the data source box that you want to edit, and verify that the following information is correct:
 - The evidence collection method is **Automated**.
 - The data source type is **AWS API calls**.
 - The selected API call is the one that you want to change the frequency for.
6. Under **Frequency**, choose how often you want to collect evidence for the custom control.
7. Repeat steps 5-6 as needed for any additional API call data sources that you want to edit.
8. Choose **Next**.
9. On the **Edit an action plan** page, choose **Next**.
10. On the **Review and update the control** page, review the information for the custom control. To change the information for a step, choose **Edit**.
11. When you're finished, choose **Save changes**.

After you edit a control with *AWS API calls* as the data source type, the changes take effect at 00:00 UTC the following day in all active assessments that include the control.

Compliance checks from AWS Config

Note

The following applies to both standard controls and custom controls that use AWS Config Rules as a data source.

If a control uses AWS Config as a data source type, you can't change the evidence collection frequency directly in Audit Manager. This is because the frequency follows the triggers that are defined in the AWS Config rule.

There are two types of triggers for AWS Config Rules:

1. **Configuration changes** - AWS Config runs evaluations for the rule when certain types of resources are created, changed, or deleted.
2. **Periodic** - AWS Config runs evaluations for the rule at a frequency that you choose (for example, every 24 hours).

To learn more about the triggers for AWS Config Rules, see [Trigger types in the AWS Config Developer Guide](#).

For instructions on how to manage AWS Config Rules, see [Managing your AWS Config rules](#).

Compliance checks from Security Hub

Note

The following applies to both standard controls and custom controls that use Security Hub checks as a data source.

If a control uses Security Hub as a data source type, you can't change the evidence collection frequency directly in Audit Manager. This is because the frequency follows the schedule of the Security Hub checks.

- **Periodic checks** run automatically within 12 hours after the most recent run. You cannot change the periodicity.
- **Change-triggered checks** run when the associated resource changes state. Even if the resource doesn't change state, the updated at time for change-triggered checks is refreshed every 18 hours. This helps to indicate that the control is still enabled. In general, Security Hub uses change-triggered rules whenever possible.

To learn more, see [Schedule for running security checks](#) in the *AWS Security Hub User Guide*.

User activity logs from AWS CloudTrail

Note

The following applies to both standard controls and custom controls that use AWS CloudTrail user activity logs as a data source.

You can't change the evidence collection frequency for controls that use activity logs from CloudTrail as a data source type. Audit Manager collects this evidence type from CloudTrail in a continuous manner. The frequency is continuous because user activity can happen at any time of the day.

Supported control data sources for automated evidence

When you create a custom control in AWS Audit Manager, you can set up your control to collect automated evidence from the following data source types:

- AWS CloudTrail
- AWS Security Hub
- AWS Config

- AWS API calls

The following topics summarize each of these automated data source types, and list the specific AWS Security Hub controls, AWS Config rules, and AWS API calls that are supported by Audit Manager.

Topics

- [Overview of automated data sources \(p. 214\)](#)
- [AWS Config Rules supported by AWS Audit Manager \(p. 215\)](#)
- [AWS Security Hub controls supported by AWS Audit Manager \(p. 224\)](#)
- [API calls supported by AWS Audit Manager \(p. 247\)](#)
- [AWS CloudTrail event names supported by AWS Audit Manager \(p. 249\)](#)

Overview of automated data sources

The following table provides an overview of each automated data source type.

Data source type	Description	Evidence collection frequency	To use this data source type...	When this control is active in an assessment...	Related troubleshooting tips
AWS CloudTrail	Tracks a specific user activity.	Continuous.	Select from the list of supported event names .	Audit Manager filters your CloudTrail logs based on the keyword that you choose. The results are imported as User activity evidence.	My assessment isn't collecting user activity evidence from AWS CloudTrail (p. 276)
AWS Config	Captures a snapshot of your resource security posture by reporting findings from AWS Config.	Based on the triggers defined in the AWS Config rule.	<p>Choose a rule type, then select a rule.</p> <ul style="list-style-type: none"> For managed rules, select from the list of supported managed rule keywords. For custom rules, select from the list of your available rules. 	Audit Manager gets the findings for this rule directly from AWS Config. The result is imported as Compliance check evidence.	My assessment isn't collecting compliance check evidence from AWS Config (p. 274) AWS Config integration issues
AWS Security Hub	Captures a snapshot of your resource security posture by reporting	Based on the schedule of the Security Hub check.	Select from the list of supported Security Hub control IDs .	Audit Manager gets the result of the security check directly from Security Hub. The result is imported as Compliance check evidence.	My assessment isn't collecting compliance check evidence

Data source type	Description	Evidence collection frequency	To use this data source type...	When this control is active in an assessment...	Related troubleshooting tips
	findings from Security Hub.				from AWS Security Hub (p. 273)
AWS API calls	Takes a snapshot of your resource configuration directly through an API call to the specified AWS service.	Daily, weekly, or monthly.	Select from the list of supported API calls , then select your preferred frequency.	Audit Manager makes the API call based on the frequency that you specify. The response is imported as Configuration data evidence.	My assessment isn't collecting configuration data evidence for an AWS API call (p. 276)

AWS Config Rules supported by AWS Audit Manager

You can use Audit Manager to capture AWS Config evaluations as evidence for audits. When you create or edit a custom control, you can specify one or more AWS Config rules as a data source mapping for evidence collection. AWS Config performs compliance checks based on these rules, and Audit Manager reports the results as compliance check evidence.

In addition to managed rules, you can also map your custom rules to a control data source.

Note

- Audit Manager doesn't collect evidence from [service-linked AWS Config rules](#), with the exception of service-linked rules from Conformance Packs and from AWS Organizations. For more information, see the [Troubleshooting](#) section of this guide.
- Audit Manager doesn't manage AWS Config rules for you. Before you start evidence collection, we recommend that you review your current AWS Config rule parameters. Then, validate those parameters against the requirements of your chosen framework. If needed, you can [update a rule's parameters in AWS Config](#) so that it aligns with framework requirements. This will help to ensure that your assessments collect the correct compliance check evidence for that framework.

For example, suppose that you're creating an assessment for CIS v1.2.0. This framework has a control named [1.9 – Ensure IAM password policy requires a minimum length of 14 or greater](#). In AWS Config, the [iam-password-policy](#) rule has a MinimumPasswordLength parameter that checks password length. The default value for this parameter is 14 characters. As a result, the rule aligns with the control requirements. If you aren't using the default parameter value, ensure that the value you're using is equal to or greater than the 14 character requirement from CIS v1.2.0. You can find the default parameter details for each managed rule in the [AWS Config documentation](#).

Topics

- [Using AWS Config managed rules with Audit Manager \(p. 216\)](#)
- [Using AWS Config custom rules with Audit Manager \(p. 223\)](#)

- [Troubleshooting AWS Config integration with Audit Manager \(p. 224\)](#)

Using AWS Config managed rules with Audit Manager

326 AWS Config managed rules are currently supported by Audit Manager. You can use any of the following managed rule identifier keywords when you set up a data source for a custom control. For more information about any of the managed rules listed below, choose an item from the list or see [AWS Config Managed Rules](#) in the *AWS Config User Guide*.

Tip

When you choose a managed rule in the Audit Manager console during custom control creation, make sure that you look for one of the following rule identifier keywords, and not the rule name. For information about the difference between the rule name and rule identifier, and how to find the identifier for a managed rule, see the [Troubleshooting](#) section of this user guide.

Supported AWS Config managed rule keywords

- [ACCESS_KEYS_ROTATED](#)
- [ACCOUNT_PART_OF_ORGANIZATIONS](#)
- [ACM_CERTIFICATE_EXPIRATION_CHECK](#)
- [ACM_CERTIFICATE_RSA_CHECK](#)
- [ALB_DESYNC_MODE_CHECK](#)
- [ALB_HTTP_DROP_INVALID_HEADER_ENABLED](#)
- [ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK](#)
- [ALB_WAF_ENABLED](#)
- [API_GW_ASSOCIATED_WITH_WAF](#)
- [API_GW_CACHE_ENABLED_AND_ENCRYPTED](#)
- [API_GW_ENDPOINT_TYPE_CHECK](#)
- [API_GW_EXECUTION_LOGGING_ENABLED](#)
- [API_GW_SSL_ENABLED](#)
- [API_GW_XRAY_ENABLED](#)
- [API_GWV2_ACCESS_LOGS_ENABLED](#)
- [API_GWV2_AUTHORIZATION_TYPE_CONFIGURED](#)
- [APPROVED_AMIS_BY_ID](#)
- [APPROVED_AMIS_BY_TAG](#)
- [APPSYNC_ASSOCIATED_WITH_WAF](#)
- [APPSYNC_CACHE_ENCRYPTION_AT_REST](#)
- [APPSYNC_LOGGING_ENABLED](#)
- [AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED](#)
- [AURORA_MYSQL_BACKTRACKING_ENABLED](#)
- [AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN](#)
- [AUTOSCALING_CAPACITY_REBALANCING](#)
- [AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED](#)
- [AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT](#)
- [AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED](#)
- [AUTOSCALING_LAUNCHCONFIGQUIRES_IMDSV2](#)
- [AUTOSCALING_LAUNCH_TEMPLATE](#)
- [AUTOSCALING_MULTIPLE_AZ](#)
- [AUTOSCALING_MULTIPLE_INSTANCE_TYPES](#)

Supported AWS Config managed rule keywords

- [BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK](#)
- [BACKUP_RECOVERY_POINT_ENCRYPTED](#)
- [BACKUP_RECOVERY_POINT_MANUAL_DELETION_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_ENABLED](#)
- [CLOUD_TRAIL_ENCRYPTION_ENABLED](#)
- [CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED](#)
- [CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK](#)
- [CLOUDFORMATION_STACK_NOTIFICATION_CHECK](#)
- [CLOUDFRONT_ACCESSLOGS_ENABLED](#)
- [CLOUDFRONT_ASSOCIATED_WITH_WAF](#)
- [CLOUDFRONT_CUSTOM_SSL_CERTIFICATE](#)
- [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_ENABLED](#)
- [CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED](#)
- [CLOUDFRONT_VIEWER_POLICY_HTTPS](#)
- [CLOUDTRAIL_S3_DATAEVENTS_ENABLED](#)
- [CLOUDTRAIL_SECURITY_TRAIL_ENABLED](#)
- [CLOUDWATCH_ALARM_ACTION_CHECK](#)
- [CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK](#)
- [CLOUDWATCH_ALARM_RESOURCE_CHECK](#)
- [CLOUDWATCH_ALARM_SETTINGS_CHECK](#)
- [CLOUDWATCH_LOG_GROUP_ENCRYPTED](#)
- [CMK_BACKING_KEY_ROTATION_ENABLED](#)
- [CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION](#)
- [CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK](#)
- [CODEBUILD_PROJECT_ENVVAR_AWSCREDS_CHECK](#)
- [CODEBUILD_PROJECT_LOGGING_ENABLED](#)
- [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](#)

Supported AWS Config managed rule keywords

- [CODEPIPELINE_REGION_FANOUT_CHECK](#)
- [CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED](#)
- [CW_LOGGROUP_RETENTION_PERIOD_CHECK](#)
- [DAX_ENCRYPTION_ENABLED](#)
- [DB_INSTANCE_BACKUP_ENABLED](#)
- [DESIRED_INSTANCE_TENANCY](#)
- [DESIRED_INSTANCE_TYPE](#)
- [DMS_REPLICATION_NOT_PUBLIC](#)
- [DYNAMODB_AUTOSCALING_ENABLED](#)
- [DYNAMODB_IN_BACKUP_PLAN](#)
- [DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED](#)
- [DYNAMODB_PITR_ENABLED](#)
- [DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN](#)
- [DYNAMODB_TABLE_ENCRYPTED_KMS](#)
- [DYNAMODB_TABLE_ENCRYPTION_ENABLED](#)
- [DYNAMODB_THROUGHPUT_LIMIT_CHECK](#)
- [EBS_IN_BACKUP_PLAN](#)
- [EBS_LAST_BACKUP_RECOVERY_POINT_CREATED](#)
- [EBS_OPTIMIZED_INSTANCE](#)
- [EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN](#)
- [EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK](#)
- [EC2_CLIENT_VPN_NOT_AUTHORIZE_ALL](#)
- [EC2_EBS_ENCRYPTION_BY_DEFAULT](#)
- [EC2_IMDSV2_CHECK](#)
- [EC2_INSTANCE_DETAILED_MONITORING_ENABLED](#)
- [EC2_INSTANCE_MANAGED_BY_SSM](#)
- [EC2_INSTANCE_MULTIPLE_ENI_CHECK](#)
- [EC2_INSTANCE_NO_PUBLIC_IP](#)
- [EC2_INSTANCE_PROFILE_ATTACHED](#)
- [EC2_LAST_BACKUP_RECOVERY_POINT_CREATED](#)
- [EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED](#)
- [EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED](#)
- [EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED](#)
- [EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK](#)
- [EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED](#)
- [EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK](#)
- [EC2_MANAGEDINSTANCE_PLATFORM_CHECK](#)
- [EC2_NO_AMAZON_KEY_PAIR](#)
- [EC2_PARAVIRTUAL_INSTANCE_CHECK](#)
- [EC2_RESOURCES_PROTECTED_BY_BACKUP_PLAN](#)
- [EC2_SECURITY_GROUP_ATTACHED_TO_ENI](#)
- [EC2_SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC](#)
- [EC2_STOPPED_INSTANCE](#)
- [EC2_TOKEN_HOP_LIMIT_CHECK](#)

Supported AWS Config managed rule keywords

- [EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED](#)
- [EC2_VOLUME_INUSE_CHECK](#)
- [ECR_PRIVATE_IMAGE_SCANNING_ENABLED](#)
- [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_LATEST_PLATFORM_VERSION](#)
- [ECS_NO_ENVIRONMENT_SECRETS](#)
- [ECS_TASK_DEFINITION_LOG_CONFIGURATION](#)
- [ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT](#)
- [ECS_TASK_DEFINITION_NONROOT_USER](#)
- [ECS_TASK_DEFINITION_PID_MODE_CHECK](#)
- [ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK](#)
- [EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY](#)
- [EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY](#)
- [EFS_ENCRYPTED_CHECK](#)
- [EFS_IN_BACKUP_PLAN](#)
- [EFS_LAST_BACKUP_RECOVERY_POINT_CREATED](#)
- [EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN](#)
- [EIP_ATTACHED](#)
- [EKS_CLUSTER_LOGGING_ENABLED](#)
- [EKS_CLUSTER_OLEDEST_SUPPORTED_VERSION](#)
- [EKS_CLUSTER_SUPPORTED_VERSION](#)
- [EKS_ENDPOINT_NO_PUBLIC_ACCESS](#)
- [EKS_SECRETS_ENCRYPTED](#)
- [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](#)
- [ELASTICACHE_SUPPORTED_ENGINE_VERSION](#)
- [ELASTICSEARCH_ENCRYPTED_AT_REST](#)
- [ELASTICSEARCH_IN_VPC_ONLY](#)
- [ELASTICSEARCH_LOGS_TO_CLOUDWATCH](#)
- [ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK](#)
- [ELB_ACN_CERTIFICATE_REQUIRED](#)

Supported AWS Config managed rule keywords

- [ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED](#)
- [ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK](#)
- [ELB_DELETION_PROTECTION_ENABLED](#)
- [ELB_LOGGING_ENABLED](#)
- [ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK](#)
- [ELB_TLS_HTTPS_LISTENERS_ONLY](#)
- [ELBV2_ACM_CERTIFICATE_REQUIRED](#)
- [ELBV2_MULTIPLE_AZ](#)
- [EMR_KERBEROS_ENABLED](#)
- [EMR_MASTER_NO_PUBLIC_IP](#)
- [ENCRYPTED_VOLUMES](#)
- [FMS_SHIELD_RESOURCE_POLICY_CHECK](#)
- [FMS_WEBACL_RESOURCE_POLICY_CHECK](#)
- [FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK](#)
- [FSX_LAST_BACKUP_RECOVERY_POINT_CREATED](#)
- [FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN](#)
- [GUARDDUTY_ENABLED_CENTRALIZED](#)
- [GUARDDUTY_NON_ARCHIVED_FINDINGS](#)
- [IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS](#)
- [IAM_GROUP_HAS_USERS_CHECK](#)
- [IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS](#)
- [IAM_NO_INLINE_POLICY_CHECK](#)
- [IAM_PASSWORD_POLICY](#)
- [IAM_POLICY_BLACKLISTED_CHECK](#)
- [IAM_POLICY_IN_USE](#)
- [IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS](#)
- [IAM_POLICY_NO_STATEMENTS_WITH_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_IN_VPC](#)
- [KINESIS_STREAM_ENCRYPTED](#)
- [INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY](#)
- [KMS_CMK_NOT_SCHEDULED_FOR_DELETION](#)
- [LAMBDA_CONCURRENCY_CHECK](#)
- [LAMBDA_DLQ_CHECK](#)
- [LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED](#)
- [LAMBDA_FUNCTION_SETTINGS_CHECK](#)
- [LAMBDA_INSIDE_VPC](#)
- [LAMBDA_VPC_MULTI_AZ_CHECK](#)

Supported AWS Config managed rule keywords

- [MACIE_STATUS_CHECK](#)
- [MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS](#)
- [MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED](#)
- [MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED](#)
- [MQ_NO_PUBLIC_ACCESS](#)
- [MULTI_REGION_CLOUD_TRAIL_ENABLED](#)
- [NACL_NO_UNRESTRICTED_SSH_RDP](#)
- [NETFW_LOGGING_ENABLED](#)
- [NETFW_MULTI_AZ_ENABLED](#)
- [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_UNRESTRICTED_ROUTE_TO_IGW](#)
- [OPENSEARCH_ACCESS_CONTROL_ENABLED](#)
- [OPENSEARCH_AUDIT_LOGGING_ENABLED](#)
- [OPENSEARCH_DATA_NODEFAULT_TOLERANCE](#)
- [OPENSEARCH_ENCRYPTED_AT_REST](#)
- [OPENSEARCH_HTTPS_REQUIRED](#)
- [OPENSEARCH_IN_VPC_ONLY](#)
- [OPENSEARCH_LOGS_TO_CLOUDWATCH](#)
- [OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK](#)
- [RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED](#)
- [RDS_CLUSTER_DEFAULT_ADMIN_CHECK](#)
- [RDS_CLUSTER_DELETION_PROTECTION_ENABLED](#)
- [RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED](#)
- [RDS_CLUSTER_MULTI_AZ_ENABLED](#)
- [RDS_DB_SECURITY_GROUP_NOT_ALLOWED](#)
- [RDS_ENHANCED_MONITORING_ENABLED](#)
- [RDS_IN_BACKUP_PLAN](#)
- [RDS_INSTANCE_DEFAULT_ADMIN_CHECK](#)
- [RDS_INSTANCE_DELETION_PROTECTION_ENABLED](#)
- [RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED](#)
- [RDS_INSTANCE_PUBLIC_ACCESS_CHECK](#)
- [RDS_LAST_BACKUP_RECOVERY_POINT_CREATED](#)
- [RDS_LOGGING_ENABLED](#)
- [RDS_MULTI_AZ_SUPPORT](#)
- [RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN](#)
- [RDS_SNAPSHOT_ENCRYPTED](#)
- [RDS_SNAPSHOTS_PUBLIC_PROHIBITED](#)
- [RDS_STORAGE_ENCRYPTED](#)
- [REDSHIFT_BACKUP_ENABLED](#)
- [REDSHIFT_REQUIRE_TLS_SSL](#)

Supported AWS Config managed rule keywords

- [REDSHIFT_CLUSTER_CONFIGURATION_CHECK](#)
- [REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK](#)
- [REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK](#)
- [REDSHIFT_AUDIT_LOGGING_ENABLED](#)
- [REDSHIFT_CLUSTER_KMS_ENABLED](#)
- [REDSHIFT_DEFAULT_ADMIN_CHECK](#)
- [REDSHIFT_DEFAULT_DB_NAME_CHECK](#)
- [REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED](#)
- [REQUIRED_TAGS](#)
- [RESTRICTED_INCOMING_TRAFFIC](#)
- [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_PROHIBITED](#)
- [S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED](#)
- [S3_BUCKET_DEFAULT_LOCK_ENABLED](#)
- [S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED](#)
- [S3_BUCKET_LOGGING_ENABLED](#)
- [S3_BUCKET_POLICY_GRANTEE_CHECK](#)
- [S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE](#)
- [S3_BUCKET_PUBLIC_READ_PROHIBITED](#)
- [S3_BUCKET_PUBLIC_WRITE_PROHIBITED](#)
- [S3_BUCKET_REPLICATION_ENABLED](#)
- [S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED](#)
- [S3_BUCKET_SSL_REQUESTS_ONLY](#)
- [S3_BUCKET_VERSIONING_ENABLED](#)
- [S3_DEFAULT_ENCRYPTION_KMS](#)
- [S3_EVENT_NOTIFICATIONS_ENABLED](#)
- [S3_LAST_BACKUP_RECOVERY_POINT_CREATED](#)
- [S3_LIFECYCLE_POLICY_CHECK](#)
- [S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN](#)
- [S3_VERSION_LIFECYCLE_POLICY_CHECK](#)
- [SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED](#)
- [SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC](#)
- [SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED](#)
- [SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK](#)
- [SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS](#)
- [SECRETSMANAGER_ROTATION_ENABLED_CHECK](#)
- [SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK](#)
- [SECRETSMANAGER_SECRET_PERIODIC_ROTATION](#)
- [SECRETSMANAGER_SECRET_UNUSED](#)
- [SECRETSMANAGER_USING_CMK](#)
- [SECURITY_ACCOUNT_INFORMATION PROVIDED](#)

Supported AWS Config managed rule keywords

- [SECURITYHUB_ENABLED](#)
- [SERVICE_VPC_ENDPOINT_ENABLED](#)
- [SES_MALWARE_SCANNING_ENABLED](#)
- [SHIELD_ADVANCED_ENABLED_AUTORENEW](#)
- [SHIELD_DRT_ACCESS](#)
- [SNS_ENCRYPTED_KMS](#)
- [SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED](#)
- [SSM_DOCUMENT_NOT_PUBLIC](#)
- [STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED](#)
- [STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED](#)
- [STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN](#)
- [SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED](#)
- [VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED](#)
- [VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN](#)
- [VPC_DEFAULT_SECURITY_GROUP_CLOSED](#)
- [VPC_FLOW_LOGS_ENABLED](#)
- [VPC_NETWORK_ACL_UNUSED_CHECK](#)
- [VPC_PEERING_DNS_RESOLUTION_CHECK](#)
- [VPC_SG_OPEN_ONLY_TOAUTHORIZED_PORTS](#)
- [VPC_VPN_2_TUNNELS_UP](#)
- [WAF_CLASSIC_LOGGING_ENABLED](#)
- [WAF_GLOBAL_RULEGROUP_NOT_EMPTY](#)
- [WAF_GLOBAL_RULE_NOT_EMPTY](#)
- [WAF_GLOBAL_WEBACL_NOT_EMPTY](#)
- [WAF_REGIONAL_RULEGROUP_NOT_EMPTY](#)
- [WAF_REGIONAL_RULE_NOT_EMPTY](#)
- [WAF_REGIONAL_WEBACL_NOT_EMPTY](#)
- [WAFV2_LOGGING_ENABLED](#)
- [WAFV2_RULEGROUP_NOT_EMPTY](#)
- [WAFV2_WEBACL_NOT_EMPTY](#)

Using AWS Config custom rules with Audit Manager

You can now use AWS Config custom rules as a data source for audit reporting. When a control has a data source that's mapped to an AWS Config rule, Audit Manager adds the evaluation that was created by the AWS Config rule.

The custom rules that you can use depend on the AWS account that you sign in to Audit Manager with. If you can access a custom rule in AWS Config, you can use it as a data source mapping in Audit Manager.

- **For individual AWS accounts** – You can use any of the custom rules that you created with your account.
- **For accounts that are part of an organization** – Either, you can use any of your member-level custom rules. Or, you can use any of the organization-level custom rules that are available to you in AWS Config.

For instructions on how to create a control that uses custom rules as a data source, see [Creating a new control from scratch](#) and [Customizing an existing control](#).

Tip

Keep in mind that managed rules aren't shown in the dropdown list of custom rules in Audit Manager.

If you want to verify if an AWS Config rule is a managed rule or a custom rule, you can do this using the [AWS Config console](#). From the left navigation menu, choose **Rules** and look for the rule in the table. If it's a managed rule, the **Type** column shows **AWS managed**.

Name	Remediation action	Type	Compliance
account-part-of-organizations	Not set	AWS managed	Compliant

To map a managed rule as a data source, you can look for the managed rule identifier keyword in Audit Manager in the dropdown list of managed rules. For more information, see the [Troubleshooting](#) section of this guide.

After you map your custom rules as a data source for a control, you can associate that control with a custom framework in Audit Manager. For instructions on how to create a custom framework that uses your custom control, see [Creating a new framework from scratch](#) and [Customizing an existing framework](#). For instructions on how to add your control to an existing custom framework, see [Editing an existing framework](#).

For information about creating a custom rule in AWS Config, see [Developing a custom rule for AWS Config](#) in the *AWS Config Developer Guide*.

Troubleshooting AWS Config integration with Audit Manager

To find answers to common questions and issues, see [AWS Config integration](#) in the *Troubleshooting* section of this guide.

AWS Security Hub controls supported by AWS Audit Manager

Audit Manager enables you to report the results of compliance checks directly from Security Hub. To do this, you specify one or more Security Hub controls as a data source mapping when you configure a custom control in Audit Manager.

Note

- Audit Manager doesn't collect evidence from [service-linked AWS Config rules that are created by Security Hub](#). For more information, see the [Troubleshooting](#) section of this guide.
- On November 9, 2022, Security Hub launched automated security checks aligned to the Center for Internet Security's (CIS) AWS Foundations Benchmark version 1.4.0 requirements, Level 1 and 2 (CIS v1.4.0). In Security Hub, the [CIS v1.4.0 standard](#) is supported in addition to the [CIS v1.2.0 standard](#).

Topics

- [Using Security Hub controls with Audit Manager \(p. 225\)](#)
- [Supported Security Hub controls \(p. 232\)](#)

Using Security Hub controls with Audit Manager

Tip

We recommend that you turn on the [consolidated control findings](#) setting in Security Hub if it's not turned on already. If you enable Security Hub on or after February 23, 2003, this setting is turned *on* by default.

When consolidated findings is enabled, Security Hub produces a single finding for each security check (even when the same check applies to multiple standards). Each Security Hub finding is collected as one unique resource assessment in Audit Manager. As a result, consolidated findings results in a decrease of the total unique resource assessments that Audit Manager performs for Security Hub findings. For this reason, using consolidated findings can often result in a reduction in your Audit Manager usages costs, without sacrificing evidence quality and availability. For more information about pricing, see [AWS Audit Manager Pricing](#).

Examples of evidence when consolidated findings is turned on or off

The following examples show a comparison of how Audit Manager collects and presents evidence depending on your Security Hub settings.

When consolidated findings is turned on

Let's say that you have enabled the following three security standards in Security Hub: AWS FSBP, PCI DSS, and CIS Benchmark v1.2.0.

- All three of these standards use the same control ([IAM.4](#)) with the same underlying AWS Config rule ([iam-root-access-key-check](#)).
- Because the consolidated control findings setting is **turned on**, Security Hub generates one single finding for this control.
- Security Hub sends the consolidated finding to Audit Manager for this control.
- The consolidated finding counts as one unique resource assessment in Audit Manager. As a result, one single piece of evidence is added to your assessment.

Here's an example of how that evidence might look:

```
{  
    "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

Let's say that you have enabled the following three security standards in Security Hub: AWS FSBP, PCI DSS, and CIS Benchmark v1.2.0.

- All three of these standards use the same control ([IAM.4](#)) with the same underlying AWS Config rule ([iam-root-access-key-check](#)).
- Because the consolidated findings setting is **turned off**, Security Hub generates a separate finding per security check for each enabled standard (in this case, three findings).

- Security Hub sends three separate standard-specific findings to Audit Manager for this control.
- The three findings count as three unique resource assessments in Audit Manager. As a result, three separate pieces of evidence are added to your assessment.

Here's an example of how that evidence might look. Note that in this example, each of the following three payloads has the same security control ID (*SecurityControlId*: "IAM.4"). For this reason, the assessment control that collects this evidence in Audit Manager (IAM.4) receives three separate pieces of evidence when the following findings come in from Security Hub.

Evidence for 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/8e2e05a2-4d50-4c2ea78f-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": {  
                    "Type": "AWS",  
                    "Value": "AWS Foundational Security Best Practices"  
                }  
            }  
        ]  
    }  
}
```

```

        "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-67ccb1c4",
        "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"
}
]
}
}

```

Evidence for 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-67ccb1c4",
                "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"
}
]
}
]
```

Evidence for 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",
            }
        ]
    }
}
```

```

    "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/PCI-DSS"
    ],
    "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/remediation"
        }
    },
    "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-67ccb1c4",
        "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/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/pci-dss/v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b"
    },
    "Resources": [
    ],
    "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"
}
]
}
}

```

Supported Security Hub controls

The following Security Hub controls are currently supported by Audit Manager. You can use any of the following standard-specific control ID keywords when you set up a data source for a custom control.

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
CIS v1.2.0	1.1	IAM.20 , CloudWatch.1
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
CIS v1.2.0	1.13	IAM.9

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
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
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

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
CIS v1.2.0	4.3	EC2.2
PCI DSS	PCI.AutoScaling.1	AutoScaling.1
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
PCI DSS	PCI.ELBv2.1	ELB.1
PCI DSS	PCI.ES.1	ES.1
PCI DSS	PCI.ES.2	ES.2
PCI DSS	PCI.GuardDuty.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.IAM.8.

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
PCI DSS	PCI.KMS.1	PCI.KMS.4
PCI DSS	PCI.Lambda.1	Lambda.1
PCI DSS	PCI.Lambda.2	Lambda.3
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
AWS Foundational Security Best Practices	Account.1	Account.1
AWS Foundational Security Best Practices	ACM.1	ACM.1
AWS Foundational Security Best Practices	ACM.2	ACM.2
AWS Foundational Security Best Practices	APIGateway.1	APIGateway.1
AWS Foundational Security Best Practices	APIGateway.2	APIGateway.2
AWS Foundational Security Best Practices	APIGateway.3	APIGateway.3
AWS Foundational Security Best Practices	APIGateway.4	APIGateway.4

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	APIGateway.5	APIGateway.5
AWS Foundational Security Best Practices	APIGateway.8	APIGateway.8
AWS Foundational Security Best Practices	APIGateway.9	APIGateway.9
AWS Foundational Security Best Practices	AppSync.2	AppSync.2
AWS Foundational Security Best Practices	AutoScaling.1	AutoScaling.1
AWS Foundational Security Best Practices	AutoScaling.2	AutoScaling.2
AWS Foundational Security Best Practices	AutoScaling.3	AutoScaling.3
AWS Foundational Security Best Practices	AutoScaling.4	AutoScaling.4
AWS Foundational Security Best Practices	Autoscaling.5	Autoscaling.5
AWS Foundational Security Best Practices	AutoScaling.6	AutoScaling.6
AWS Foundational Security Best Practices	AutoScaling.9	AutoScaling.9
AWS Foundational Security Best Practices	CloudFormation.1	CloudFormation.1
AWS Foundational Security Best Practices	CloudFront.1	CloudFront.1
AWS Foundational Security Best Practices	CloudFront.2	CloudFront.2
AWS Foundational Security Best Practices	CloudFront.3	CloudFront.3
AWS Foundational Security Best Practices	CloudFront.4	CloudFront.4
AWS Foundational Security Best Practices	CloudFront.5	CloudFront.5
AWS Foundational Security Best Practices	CloudFront.6	CloudFront.6

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	CloudFront.7	CloudFront.7
AWS Foundational Security Best Practices	CloudFront.8	CloudFront.8
AWS Foundational Security Best Practices	CloudFront.9	CloudFront.9
AWS Foundational Security Best Practices	CloudFront.10	CloudFront.10
AWS Foundational Security Best Practices	CloudFront.12	CloudFront.12
AWS Foundational Security Best Practices	CloudFront.13	CloudFront.13
AWS Foundational Security Best Practices	CloudTrail.1	CloudTrail.1
AWS Foundational Security Best Practices	CloudTrail.2	CloudTrail.2
AWS Foundational Security Best Practices	CloudTrail.4	CloudTrail.4
AWS Foundational Security Best Practices	CloudTrail.5	CloudTrail.5
AWS Foundational Security Best Practices	CodeBuild.1	CodeBuild.1
AWS Foundational Security Best Practices	CodeBuild.2	CodeBuild.2
AWS Foundational Security Best Practices	CodeBuild.3	CodeBuild.3
AWS Foundational Security Best Practices	CodeBuild.4	CodeBuild.4
AWS Foundational Security Best Practices	CodeBuild.5	CodeBuild.5
AWS Foundational Security Best Practices	Config.1	Config.1
AWS Foundational Security Best Practices	DMS.1	DMS.1
AWS Foundational Security Best Practices	DynamoDB.1	DynamoDB.1

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	DynamoDB.2	DynamoDB.2
AWS Foundational Security Best Practices	DynamoDB.3	DynamoDB.3
AWS Foundational Security Best Practices	EC2.1	EC2.1
AWS Foundational Security Best Practices	EC2.2	EC2.2
AWS Foundational Security Best Practices	EC2.3	EC2.3
AWS Foundational Security Best Practices	EC2.4	EC2.4
AWS Foundational Security Best Practices	EC2.6	EC2.6
AWS Foundational Security Best Practices	EC2.7	EC2.7
AWS Foundational Security Best Practices	EC2.8	EC2.8
AWS Foundational Security Best Practices	EC2.9	EC2.9
AWS Foundational Security Best Practices	EC2.10	EC2.10
AWS Foundational Security Best Practices	EC2.15	EC2.15
AWS Foundational Security Best Practices	EC2.16	EC2.16
AWS Foundational Security Best Practices	EC2.17	EC2.17
AWS Foundational Security Best Practices	EC2.18	EC2.18
AWS Foundational Security Best Practices	EC2.19	EC2.19
AWS Foundational Security Best Practices	EC2.20	EC2.20
AWS Foundational Security Best Practices	EC2.21	EC2.21

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	EC2.22	EC2.22
AWS Foundational Security Best Practices	EC2.23	EC2.23
AWS Foundational Security Best Practices	EC2.24	EC2.24
AWS Foundational Security Best Practices	EC2.25	EC2.25
AWS Foundational Security Best Practices	ECR.1	ECR.1
AWS Foundational Security Best Practices	ECR.2	ECR.2
AWS Foundational Security Best Practices	ECR.3	ECR.3
AWS Foundational Security Best Practices	ECS.1	ECS.1
AWS Foundational Security Best Practices	ECS.2	ECS.2
AWS Foundational Security Best Practices	ECS.3	ECS.3
AWS Foundational Security Best Practices	ECS.4	ECS.4
AWS Foundational Security Best Practices	ECS.5	ECS.5
AWS Foundational Security Best Practices	ECS.8	ECS.8
AWS Foundational Security Best Practices	ECS.10	ECS.10
AWS Foundational Security Best Practices	ECS.12	ECS.12
AWS Foundational Security Best Practices	EFS.1	EFS.1
AWS Foundational Security Best Practices	EFS.2	EFS.2
AWS Foundational Security Best Practices	EFS.3	EFS.3

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	EFS.4	EFS.4
AWS Foundational Security Best Practices	EKS.1	EKS.1
AWS Foundational Security Best Practices	EKS.2	EKS.2
AWS Foundational Security Best Practices	ElasticBeanstalk.1	ElasticBeanstalk.1
AWS Foundational Security Best Practices	ElasticBeanstalk.2	ElasticBeanstalk.2
AWS Foundational Security Best Practices	ElasticBeanstalk.3	ElasticBeanstalk.3
AWS Foundational Security Best Practices	ELB.2	ELB.2
AWS Foundational Security Best Practices	ELB.3	ELB.3
AWS Foundational Security Best Practices	ELB.4	ELB.4
AWS Foundational Security Best Practices	ELB.5	ELB.5
AWS Foundational Security Best Practices	ELB.6	ELB.6
AWS Foundational Security Best Practices	ELB.7	ELB.7
AWS Foundational Security Best Practices	ELB.8	ELB.8
AWS Foundational Security Best Practices	ELB.9	ELB.9
AWS Foundational Security Best Practices	ELB.10	ELB.10
AWS Foundational Security Best Practices	ELB.12	ELB.12
AWS Foundational Security Best Practices	ELB.13	ELB.13
AWS Foundational Security Best Practices	ELB.14	ELB.14

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	ELBv2.1	ELB.1
AWS Foundational Security Best Practices	EMR.1	EMR.1
AWS Foundational Security Best Practices	ES.1	ES.1
AWS Foundational Security Best Practices	ES.2	ES.2
AWS Foundational Security Best Practices	ES.3	ES.3
AWS Foundational Security Best Practices	ES.4	ES.4
AWS Foundational Security Best Practices	ES.5	ES.5
AWS Foundational Security Best Practices	ES.6	ES.6
AWS Foundational Security Best Practices	ES.7	ES.7
AWS Foundational Security Best Practices	ES.8	ES.8
AWS Foundational Security Best Practices	GuardDuty.1	GuardDuty.1
AWS Foundational Security Best Practices	IAM.1	IAM.1
AWS Foundational Security Best Practices	IAM.2	IAM.2
AWS Foundational Security Best Practices	IAM.3	IAM.3
AWS Foundational Security Best Practices	IAM.4	IAM.4
AWS Foundational Security Best Practices	IAM.5	IAM.5
AWS Foundational Security Best Practices	IAM.6	IAM.6
AWS Foundational Security Best Practices	IAM.7	IAM.7

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	IAM.8	IAM.8
AWS Foundational Security Best Practices	IAM.21	IAM.21
AWS Foundational Security Best Practices	Kinesis.1	Kinesis.1
AWS Foundational Security Best Practices	KMS.1	KMS.1
AWS Foundational Security Best Practices	KMS.2	KMS.2
AWS Foundational Security Best Practices	KMS.3	KMS.3
AWS Foundational Security Best Practices	Lambda.1	Lambda.1
AWS Foundational Security Best Practices	Lambda.2	Lambda.2
AWS Foundational Security Best Practices	Lambda.5	Lambda.5
AWS Foundational Security Best Practices	NetworkFirewall.3	NetworkFirewall.3
AWS Foundational Security Best Practices	NetworkFirewall.4	NetworkFirewall.4
AWS Foundational Security Best Practices	NetworkFirewall.5	NetworkFirewall.5
AWS Foundational Security Best Practices	NetworkFirewall.6	NetworkFirewall.6
AWS Foundational Security Best Practices	Opensearch.1	Opensearch.1
AWS Foundational Security Best Practices	Opensearch.2	Opensearch.2
AWS Foundational Security Best Practices	Opensearch.3	Opensearch.3
AWS Foundational Security Best Practices	Opensearch.4	Opensearch.4
AWS Foundational Security Best Practices	Opensearch.5	Opensearch.5

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	Opensearch.6	Opensearch.6
AWS Foundational Security Best Practices	Opensearch.7	Opensearch.7
AWS Foundational Security Best Practices	Opensearch.8	Opensearch.8
AWS Foundational Security Best Practices	RDS.1	RDS.1
AWS Foundational Security Best Practices	RDS.2	RDS.2
AWS Foundational Security Best Practices	RDS.3	RDS.3
AWS Foundational Security Best Practices	RDS.4	RDS.4
AWS Foundational Security Best Practices	RDS.5	RDS.5
AWS Foundational Security Best Practices	RDS.6	RDS.6
AWS Foundational Security Best Practices	RDS.7	RDS.7
AWS Foundational Security Best Practices	RDS.8	RDS.8
AWS Foundational Security Best Practices	RDS.9	RDS.9
AWS Foundational Security Best Practices	RDS.10	RDS.10
AWS Foundational Security Best Practices	RDS.11	RDS.11
AWS Foundational Security Best Practices	RDS.12	RDS.12
AWS Foundational Security Best Practices	RDS.13	RDS.13
AWS Foundational Security Best Practices	RDS.14	RDS.14
AWS Foundational Security Best Practices	RDS.15	RDS.15

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	RDS.16	RDS.16
AWS Foundational Security Best Practices	RDS.17	RDS.17
AWS Foundational Security Best Practices	RDS.18	RDS.18
AWS Foundational Security Best Practices	RDS.19	RDS.19
AWS Foundational Security Best Practices	RDS.20	RDS.20
AWS Foundational Security Best Practices	RDS.21	RDS.21
AWS Foundational Security Best Practices	RDS.22	RDS.22
AWS Foundational Security Best Practices	RDS.23	RDS.23
AWS Foundational Security Best Practices	RDS.24	RDS.24
AWS Foundational Security Best Practices	RDS.25	RDS.25
AWS Foundational Security Best Practices	Redshift.1	Redshift.1
AWS Foundational Security Best Practices	Redshift.2	Redshift.2
AWS Foundational Security Best Practices	Redshift.3	Redshift.3
AWS Foundational Security Best Practices	Redshift.4	Redshift.4
AWS Foundational Security Best Practices	Redshift.6	Redshift.6
AWS Foundational Security Best Practices	Redshift.7	Redshift.7
AWS Foundational Security Best Practices	Redshift.8	Redshift.8
AWS Foundational Security Best Practices	Redshift.9	Redshift.9

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	Redshift.10	Redshift.10
AWS Foundational Security Best Practices	S3.1	S3.1
AWS Foundational Security Best Practices	S3.2	S3.2
AWS Foundational Security Best Practices	S3.3	S3.3
AWS Foundational Security Best Practices	S3.4	S3.4
AWS Foundational Security Best Practices	S3.5	S3.5
AWS Foundational Security Best Practices	S3.6	S3.6
AWS Foundational Security Best Practices	S3.8	S3.8
AWS Foundational Security Best Practices	S3.9	S3.9
AWS Foundational Security Best Practices	S3.10	S3.10
AWS Foundational Security Best Practices	S3.11	S3.11
AWS Foundational Security Best Practices	S3.12	S3.12
AWS Foundational Security Best Practices	S3.13	S3.13
AWS Foundational Security Best Practices	SageMaker.1	SageMaker.1
AWS Foundational Security Best Practices	SageMaker.2	SageMaker.2
AWS Foundational Security Best Practices	SageMaker.3	SageMaker.3
AWS Foundational Security Best Practices	SecretsManager.1	SecretsManager.1
AWS Foundational Security Best Practices	SecretsManager.2	SecretsManager.2

Security standard	Supported keyword in Audit Manager (standard control ID in Security Hub)	Related control documentation (corresponding security control ID in Security Hub)
AWS Foundational Security Best Practices	SecretsManager.3	SecretsManager.3
AWS Foundational Security Best Practices	SecretsManager.4	SecretsManager.4
AWS Foundational Security Best Practices	SNS.1	SNS.1
AWS Foundational Security Best Practices	SNS.2	SNS.2
AWS Foundational Security Best Practices	SQS.1	SQS.1
AWS Foundational Security Best Practices	SSM.1	SSM.1
AWS Foundational Security Best Practices	SSM.2	SSM.2
AWS Foundational Security Best Practices	SSM.3	SSM.3
AWS Foundational Security Best Practices	SSM.4	SSM.4
AWS Foundational Security Best Practices	StepFunctions.1	StepFunctions.1
AWS Foundational Security Best Practices	WAF.1	WAF.1
AWS Foundational Security Best Practices	WAF.2	WAF.2
AWS Foundational Security Best Practices	WAF.3	WAF.3
AWS Foundational Security Best Practices	WAF.4	WAF.4
AWS Foundational Security Best Practices	WAF.6	WAF.6
AWS Foundational Security Best Practices	WAF.7	WAF.7
AWS Foundational Security Best Practices	WAF.8	WAF.8
AWS Foundational Security Best Practices	WAF.10	WAF.10

API calls supported by AWS Audit Manager

Audit Manager makes API calls to AWS services to collect a snapshot of the configuration details for your AWS resources. You can specify these API calls as a data source mapping when you configure a custom control in Audit Manager.

For every resource that's in the scope of an API call, Audit Manager captures a configuration snapshot and converts it into evidence. This results in one piece of evidence per resource, as opposed to one piece of evidence per API call.

For example, if the `ec2_DescribeRouteTables` API call captures configuration snapshots from five route tables, then you'll get five pieces of evidence in total for the single API call. Each piece of evidence is a snapshot of the configuration of an individual route table.

On this page

- [Supported API calls for custom control data sources \(p. 247\)](#)
- [Paginated API calls \(p. 248\)](#)
- [API calls used in the AWS License Manager standard framework \(p. 249\)](#)

Supported API calls for custom control data sources

In your custom controls, you can use any of the following 29 API calls as a data source.

Supported API call	Notes
config_DescribeConfigRules	
config_DescribeDeliveryChannels	
cloudwatch_DescribeAlarms	
cloudtrail_DescribeTrails	
dynamodb_DescribeTable	When you use this API as a data source, you don't need to provide the name of a specific DynamoDB table. Instead, Audit Manager uses the <code>ListTables</code> operation to list all of your tables. For every table that's listed, Audit Manager then performs the <code>DescribeTable</code> operation to generate evidence for that resource.
dynamodb_ListTables	
ec2_DescribeFlowLogs	
ec2_DescribeInstances	
ec2_DescribeNetworkAcls	
ec2_DescribeRouteTables	
ec2_DescribeSecurityGroups	
ec2_DescribeVolumes	
ec2_DescribeVpcs	
ec2_DescribeVpcEndpoints	
elasticfilesystem_DescribeFileSystems	

Supported API call	Notes
kms_GetKeyPolicy	When you use this API as a data source, you don't need to provide the name of a specific AWS KMS key. Instead, Audit Manager uses the ListKeys operation to list all of your KMS keys. For every KMS key that's listed, Audit Manager then performs the GetKeyPolicy operation to generate evidence for that resource.
kms_GetKeyRotationStatus	When you use this API as a data source, you don't need to provide the name of a specific AWS KMS key. Instead, Audit Manager uses the ListKeys operation to list all of your KMS keys. For every KMS key that's listed, Audit Manager then performs the GetKeyRotationStatus operation to generate evidence for that resource.
kms_ListKeys	
iam_GenerateCredentialReport	
iam_GetAccountPasswordPolicy	
iam_GetAccountSummary	
iam_ListGroups	
iam_ListPolicies	
iam_ListRoles	
iam_ListUsers	
rds_DescribeDBInstances	
redshift_DescribeClusters	
s3_GetBucketEncryption	When you use this API as a data source, you don't need to provide the name of a specific S3 bucket. Instead, Audit Manager uses the ListBuckets operation to list all of your buckets. For every bucket that's listed, Audit Manager then performs the GetBucketEncryption operation to generate evidence for that resource. Audit Manager can only provide the encryption status for buckets that were created in the same AWS Region as your assessment. If you need to see the encryption status of all your S3 buckets across multiple AWS Regions, we recommend that you create an assessment in each AWS Region where you have an S3 bucket.
s3_ListBuckets	

Paginated API calls

Many AWS services collect and store a large amount of data. As a result, when a list, describe, or get API call attempts to return your data, there can be a lot of results. If the amount of data is too large to return in a single response, the results can be broken into more manageable pieces through the use of *pagination*. This divides the results into "pages" of data, making the responses easier to handle.

Some of the [API calls that Audit Manager supports](#) are paginated. This means that they return partial results at first, and require subsequent requests to return the entire result set. For example, the Amazon RDS [DescribeDBInstances](#) operation returns up to 100 instances at a time, and subsequent requests are needed to return the next page of results.

As of March 08, 2023, Audit Manager supports paginated API calls as a data source for evidence collection. Previously, if a paginated API call was used as a data source, only a subset of your resources was returned in the API response (up to 100 results). Now, Audit Manager calls the paginated API operation multiple times, and gets each page of results until all resources are returned. For each resource, Audit Manager then captures a configuration snapshot and saves it as evidence. Because your complete set of resources is now captured in the API response, it's likely that you'll notice an increase in the amount of evidence that's collected.

Audit Manager handles API call pagination for you automatically. If you create a custom control that uses a paginated API call as a data source, you don't need to specify any pagination parameters.

API calls used in the AWS License Manager standard framework

In the [AWS License Manager](#) standard framework, Audit Manager uses a custom activity called `GetLicenseManagerSummary` to collect evidence. This activity calls the following three License Manager APIs:

- [ListLicenseConfigurations](#)
- [ListAssociationsForLicenseConfiguration](#)
- [ListUsageForLicenseConfiguration](#)

The data that's returned is then converted into evidence and attached to the relevant controls in your assessment.

Example

Let's say that you use two licensed products (*SQL Service 2017* and *Oracle Database Enterprise Edition*). First, the `GetLicenseManagerSummary` activity calls the [ListLicenseConfigurations](#) API, which provides details of license configurations in your account. Next, it adds additional contextual data for each license configuration by calling [ListUsageForLicenseConfiguration](#) and [ListAssociationsForLicenseConfiguration](#). Finally, it converts the license configuration data into evidence and attaches it to the respective controls in the framework (*4.5 - Customer managed license for SQL Server 2017* and *3.0.4 - Customer managed license for Oracle Database Enterprise Edition*).

If you're using a licensed product that isn't covered by any of the controls in the framework, that license configuration data is attached as evidence to the following control: *5.0 - Customer managed license for other licenses*.

AWS CloudTrail event names supported by AWS Audit Manager

You can capture AWS CloudTrail [management events](#) and [global service events](#) as evidence in Audit Manager. To do this, you specify the CloudTrail event name as a data source mapping keyword when you create a custom control.

Note

Audit Manager captures management events and global service events only. Data events and insights events are not available as evidence. For more information about the different types of CloudTrail events, see [CloudTrail concepts](#) in the [AWS CloudTrail User Guide](#).

As an exception to the above, the following CloudTrail events aren't supported by Audit Manager:

- `kms_GenerateDataKey`
- `kms_Decrypt`
- `sts_AssumeRole`

- kinesisvideo_GetDataEndpoint
- kinesisvideo_GetSignalingChannelEndpoint
- kinesisvideo_DescribeSignalingChannel
- kinesisvideo_DescribeStream

As of May 11, 2023, Audit Manager no longer supports read-only CloudTrail events as keywords for evidence collection. We removed a total of 3,135 read-only keywords. Because customers and AWS services both make read calls to APIs, read-only events are noisy. As a result, read-only keywords collect a lot of evidence that isn't reliable or relevant for audits. Read-only keywords include List, Describe, and Get API calls (for example, [GetObject](#) and [ListBuckets](#) for Amazon S3). If you were using one of these keywords for evidence collection, you don't need to do anything. The keywords were automatically removed from the Audit Manager console and from your assessments, and evidence is no longer collected for these keywords.

AWS Audit Manager settings

You can review and configure your AWS Audit Manager settings at any time.

To access your settings

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the left navigation pane, choose **Settings**.

The following settings are available:

- [General settings \(p. 251\)](#)
- [Permissions \(p. 251\)](#)
- [Data encryption \(p. 252\)](#)
- [Delegated administrator \(optional\) \(p. 253\)](#)
- [AWS Config \(optional\) \(p. 257\)](#)
- [Security Hub \(optional\) \(p. 258\)](#)
- [Disable AWS Audit Manager \(p. 258\)](#)
- [Assessment settings \(p. 259\)](#)
 - [Default audit owners \(optional\) \(p. 260\)](#)
 - [Assessment report destination \(optional\) \(p. 260\)](#)
 - [Notifications \(optional\) \(p. 262\)](#)
- [Evidence finder settings \(p. 263\)](#)
 - [Evidence finder \(optional\) \(p. 263\)](#)
 - [Export destination \(optional\) \(p. 267\)](#)

General settings

The **General** settings tab is the default view of the settings page in the Audit Manager console. Use this tab to review and update your general Audit Manager settings.

Topics

- [Permissions \(p. 251\)](#)
- [Data encryption \(p. 252\)](#)
- [Delegated administrator \(optional\) \(p. 253\)](#)
- [AWS Config \(optional\) \(p. 257\)](#)
- [Security Hub \(optional\) \(p. 258\)](#)
- [Disable AWS Audit Manager \(p. 258\)](#)

Permissions

AWS Audit Manager uses a service-linked role to connect to data sources on your behalf. For more information, see [Using service-linked roles for AWS Audit Manager \(p. 351\)](#).

To review the details of the service-linked role that Audit Manager uses, choose **View IAM service-linked role permission**.

For more information about service-linked roles, see [Using service-linked roles](#) in the *IAM User Guide*.

Data encryption

Audit Manager automatically creates a unique AWS managed key for the secure storage of your data. By default, your Audit Manager data is encrypted with this KMS key. Alternatively, if you want to customize your data encryption settings, you can specify your own symmetric encryption customer managed key. Using your own KMS key gives you more flexibility, including the ability to create, rotate, and disable keys.

Important

To generate assessment reports and export evidence finder search results successfully, your customer managed key (if you provide one) must be in the same AWS Region as your assessment. For a list of Audit Manager Regions, see [AWS Audit Manager endpoints and quotas](#) in the *Amazon Web Services General Reference*.

You can update your data encryption settings using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

Audit Manager console

To update your data encryption settings (console)

1. From the **General** settings tab, go to the **Data encryption** section.
2. To use the default KMS key that's provided by Audit Manager, clear the **Customize encryption settings (advanced)** check box.
3. To use a customer managed key, select the **Customize encryption settings (advanced)** check box. You can then choose an existing KMS key, or create a new one.

AWS CLI

To update your data encryption settings (AWS CLI)

Run the [update-settings](#) command and use the --kms-key parameter to specify your own customer managed key.

In the following example, replace the *placeholder text* with your own information.

```
aws auditmanager update-settings --kms-key arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Audit Manager API

To update your data encryption settings (API)

Call the [UpdateSettings](#) operation and use the [kmsKey](#) parameter to specify your own customer managed key.

For more information, choose the previous links to read more in the *Audit Manager API Reference*. This includes information about how to use this operation and parameter in one of the language-specific AWS SDKs.

Note

When you change your Audit Manager data encryption settings, these changes apply to any new assessments that you create. This includes any assessment reports and evidence finder exports that you create from your new assessments.

The changes don't apply to existing assessments that you created before you changed your encryption settings. This includes new assessment reports and CSV exports that you create from existing assessments, in addition to existing assessment reports and CSV exports. Existing assessments—and all their assessment reports and CSV exports—continue to use the old KMS key.

If the IAM identity that generates the assessment report can't use the old KMS key, grant permissions at the key policy level. For instructions, see [Allowing users in other accounts to use a KMS key](#) in the *AWS Key Management Service Developer Guide*.

For instructions on how to create keys, see [Creating keys](#) in the *AWS Key Management Service User Guide*.

Delegated administrator (optional)

If you use AWS Organizations and want to enable multi-account support for Audit Manager, you can designate a member account in your organization as the delegated administrator for Audit Manager.

Prerequisites

- Your account must be part of an organization. For more information, see [Creating and managing an organization](#) in the *AWS Organizations User Guide*.
- Before you designate a delegated administrator, you must [enable all features in your organization](#). You must also [configure your organization's Security Hub settings](#). This way, Audit Manager can collect Security Hub evidence from your member accounts.
- The delegated administrator account must have access on the KMS key that you provided when setting up Audit Manager. To review and change your encryption settings, see [Data encryption \(p. 252\)](#).

Important considerations for delegated administrators in Audit Manager

Take note of the following factors that define how the delegated administrator operates in Audit Manager:

Management account usage

You can't use your AWS Organizations management account as a delegated administrator in Audit Manager.

Using delegated administrators across multiple AWS Regions

If you want to enable Audit Manager in more than one AWS Region, you must designate a delegated administrator account separately in each Region. In your Audit Manager settings, you should use the same delegated administrator account across all Regions.

Evidence finder cleanup task

Before you use your management account to remove or change a delegated administrator, make sure that the current delegated administrator account signs in to Audit Manager and disables evidence finder. Disabling evidence finder automatically deletes the event data store that was created in the account when evidence finder was enabled.

If this task isn't completed, the event data store remains in their account. In this case, we recommend that the original delegated administrator uses CloudTrail Lake to manually [delete the event data store](#).

This cleanup task is necessary to ensure that you don't end up with multiple event data stores. Audit Manager ignores an unused event data store after you remove or change a delegated administrator account. However, if you don't delete the unused event data store, the event data store continues to incur storage costs from CloudTrail Lake.

Data deletion

When you remove a delegated administrator account for Audit Manager, the data for that account isn't deleted. If you want to delete resource data for a delegated administrator account, you must perform that task separately before you remove the account. Either, you can do this in the Audit Manager console. Or, you can use one of the delete API operations that are provided by Audit Manager. For a list of available delete operations, see [Deletion of Audit Manager data](#).

At this time, Audit Manager doesn't provide an option to delete evidence for a specific delegated administrator. Instead, when your management account deregisters Audit Manager, we perform a cleanup for the current delegated administrator account at the time of deregistration.

For solutions to common Organizations and delegated administrator issues in Audit Manager, see [Troubleshooting delegated administrator and AWS Organizations issues \(p. 289\)](#).

Managing your delegated administrator account for Audit Manager

You can review and change your delegated administrator account settings as follows.

Add a delegated administrator

You can add a delegated administrator using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

Note

After you add a delegated administrator in your Audit Manager settings, your management account can no longer create additional assessments in Audit Manager. Additionally, evidence collection stops for any existing assessments created by the management account. Audit Manager collects and attaches evidence to the delegated administrator account, which is the main account for managing your organization's assessments.

Audit Manager console

To add a delegated administrator (console)

1. From the **General** settings tab, go to the **Delegated administrator** section.
2. Under **Delegated administrator account ID**, enter the account ID of the delegated administrator.
3. Choose **Delegate**.

AWS CLI

To add a delegated administrator (AWS CLI)

Run the [register-organization-admin-account](#) command and use the `--admin-account-id` parameter to specify the account ID of the delegated administrator.

In the following example, replace the `placeholder text` with your own information.

```
aws auditmanager register-organization-admin-account --admin-account-id 111122223333
```

Audit Manager API

To add a current delegated administrator (API)

Call the [RegisterOrganizationAdminAccount](#) operation and use the [adminAccountId](#) parameter to specify the account ID of the delegated administrator.

For more information, choose the previous links to read more in the *Audit Manager API Reference*. This includes information about how to use this operation and parameter in one of the language-specific AWS SDKs.

Change a delegated administrator

You can change a delegated administrator using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

Warning

When you change a delegated administrator, you continue to have access to the evidence that you previously collected under the old delegated administrator account. However, Audit Manager stops collecting and attaching evidence to the old delegated administrator account.

Audit Manager console

To change the current delegated administrator (console)

1. (Optional) If the current delegated administrator (account A) enabled evidence finder, perform the following cleanup task:
 - Before assigning account B as the new delegated administrator, make sure that account A signs in to Audit Manager and disables evidence finder.

Disabling evidence finder automatically deletes the event data store that was created when account A enabled evidence finder. If you don't complete this step, then account A must go to CloudTrail Lake and manually [delete the event data store](#). Otherwise, the event data store remains in account A and continues to incur CloudTrail Lake storage charges.
2. From the **General** settings tab, go to the **Delegated administrator** section and choose **Remove**.
3. In the pop-up window that appears, choose **Remove** to confirm.
4. Under **Delegated administrator account ID**, enter the ID of the new delegated administrator account.
5. Choose **Delegate**.

AWS CLI

Before you start

If the current delegated administrator (account A) enabled evidence finder, perform the following cleanup task:

Before assigning account B as the new delegated administrator, make sure that account A signs in to Audit Manager and disables evidence finder.

Disabling evidence finder automatically deletes the event data store that was created when account A enabled evidence finder. If you don't complete this step, then account A must go to CloudTrail Lake and manually [delete the event data store](#). Otherwise, the event data store remains in account A and continues to incur CloudTrail Lake storage charges.

To change the current delegated administrator (AWS CLI)

First, run the [deregister-organization-admin-account](#) command using the `--admin-account-id` parameter to specify the account ID of the current delegated administrator.

In the following example, replace the *placeholder text* with your own information.

```
aws auditmanager deregister-organization-admin-account --admin-account-id 11122223333
```

Then, run the [register-organization-admin-account](#) command using the --admin-account-id parameter to specify the account ID of the new delegated administrator.

In the following example, replace the *placeholder text* with your own information.

```
aws auditmanager register-organization-admin-account --admin-account-id 444455556666
```

Audit Manager API

Before you start

If the current delegated administrator (account A) enabled evidence finder, perform the following cleanup task:

Before assigning account B as the new delegated administrator, make sure that account A signs in to Audit Manager and disables evidence finder.

Disabling evidence finder automatically deletes the event data store that was created when account A enabled evidence finder. If you don't complete this step, then account A must go to CloudTrail Lake and manually [delete the event data store](#). Otherwise, the event data store remains in account A and continues to incur CloudTrail Lake storage charges.

To change the current delegated administrator (API)

First, call the [DeregisterOrganizationAdminAccount](#) operation and use the [adminAccountId](#) parameter to specify the account ID of the current delegated administrator.

Then, call the [RegisterOrganizationAdminAccount](#) operation and use the [adminAccountId](#) parameter to specify the account ID of the new delegated administrator.

For more information, choose the previous links to read more in the *Audit Manager API Reference*. This includes information about how to use this operation and parameter in one of the language-specific AWS SDKs.

Remove a delegated administrator

You can remove a delegated administrator using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

Warning

When you remove a delegated administrator, you continue to have access to the evidence that you previously collected under that delegated administrator account. However, Audit Manager stops collecting and attaching evidence to the old delegated administrator account.

Audit Manager console

To remove the current delegated administrator (console)

1. (Optional) If the current delegated administrator enabled evidence finder, perform the following cleanup task:
 - Make sure that the current delegated administrator account signs in to Audit Manager and disables evidence finder.

Disabling evidence finder automatically deletes the event data store that was created in their account when they enabled evidence finder. If this step isn't completed, the delegated administrator account must use CloudTrail Lake to manually [delete the event data store](#).

Otherwise, the event data store remains in their account and continues to incur CloudTrail Lake storage charges.

2. From the **General** settings tab, go to the **Delegated administrator** section and choose **Remove**.
3. In the pop-up window that appears, choose **Remove** to confirm.

AWS CLI

Before you start

If the current delegated administrator enabled evidence finder, perform the following cleanup task:

Make sure that the current delegated administrator account signs in to Audit Manager and disables evidence finder.

Disabling evidence finder automatically deletes the event data store that was created in their account when they enabled evidence finder. If this step isn't completed, the delegated administrator account must use CloudTrail Lake to manually [delete the event data store](#). Otherwise, the event data store remains in their account and continues to incur CloudTrail Lake storage charges.

To remove the current delegated administrator (AWS CLI)

Run the [deregister-organization-admin-account](#) command and use the `--admin-account-id` parameter to specify the account ID of the delegated administrator.

In the following example, replace the *placeholder text* with your own information.

```
aws auditmanager deregister-organization-admin-account --admin-account-id 111122223333
```

Audit Manager API

Before you start

If the current delegated administrator enabled evidence finder, perform the following cleanup task:

Make sure that the current delegated administrator account signs in to Audit Manager and disables evidence finder.

Disabling evidence finder automatically deletes the event data store that was created in their account when they enabled evidence finder. If this step isn't completed, the delegated administrator account must use CloudTrail Lake to manually [delete the event data store](#). Otherwise, the event data store remains in their account and continues to incur CloudTrail Lake storage charges.

To remove the current delegated administrator (API)

Call the [DeregisterOrganizationAdminAccount](#) operation and use the `adminAccountId` parameter to specify the account ID of the delegated administrator.

For more information, choose the previous links to read more in the *Audit Manager API Reference*. This includes information about how to use this operation and parameter in one of the language-specific AWS SDKs.

AWS Config (optional)

You can allow Audit Manager to collect findings from AWS Config. When AWS Config is enabled, Audit Manager can capture snapshots of your resource security posture by reporting the results of rule checks directly from AWS Config. We recommend that you enable AWS Config for an optimal experience in Audit Manager.

To enable AWS Config, choose **Enable AWS Config** to go to that service. For instructions on how to enable AWS Config, see [Setting up AWS Config](#) in the *AWS Config Developer Guide*.

Security Hub (optional)

You can allow Audit Manager to import AWS Security Hub findings for supported compliance standards. When Security Hub is enabled, Audit Manager can capture snapshots of your resource security posture by the results of security checks directly from Security Hub. We recommend that you enable Security Hub for an optimal experience in Audit Manager.

To enable Security Hub, choose **Enable Security Hub** to go to that service. For instructions on how to enable Security Hub, see [Setting up AWS Security Hub](#) in the *Security Hub User Guide*.

Disable AWS Audit Manager

You can disable Audit Manager if you no longer want to use the service. When you disable Audit Manager, you also have the option to delete all of your data.

By default, your data isn't deleted when you disable Audit Manager. Your evidence data is retained for two years from the time of its creation. Your other Audit Manager resources (including assessments, custom controls, and custom frameworks) are retained indefinitely, and will be available if you re-enable Audit Manager in the future. For more information about data retention, see [Data Protection](#) in this guide.

If you choose to delete your data, Audit Manager deletes all evidence data along with all of the Audit Manager resources that you created (including assessments, custom controls, and custom frameworks). All of your data is deleted within seven days of disabling Audit Manager.

Warning

- When you disable Audit Manager, your access is revoked and the service no longer collects evidence for any existing assessments. You can't access anything in the service unless you re-enable Audit Manager.
- Deleting all data is a permanent action. If you decide to re-enable Audit Manager in the future, your data won't be recoverable.

You can disable Audit Manager using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

Audit Manager console

To disable Audit Manager (console)

- From the **General** settings tab, go to the **Disable AWS Audit Manager** section.
- Choose **Disable**.
- In the pop-up window, review your current data retention setting.
 - To proceed with your current selection, choose **Disable Audit Manager**.
 - To change your current selection, perform the following steps:
 - Choose **Cancel** to return to the settings page.
 - To use the default data retention setting, turn off **Delete all data**. This selection retains evidence data for two years from the time of its creation, and retains other Audit Manager resources indefinitely.
 - To delete your data, turn on **Delete all data**.
 - Choose **Disable**, and then choose **Disable Audit Manager** to confirm your choice.

AWS CLI

Before you start

Before you disable Audit Manager, you can run the [update-settings](#) command to set your preferred data retention policy. By default, Audit Manager retains your data. If you want to request the deletion of your data, use the --deregistration-policy parameter with the deleteResources value set to ALL.

```
aws auditmanager update-settings --deregistration-policy deleteResources=ALL
```

To disable Audit Manager (AWS CLI)

When you're ready to disable Audit Manager, run the [deregister-account](#) command.

```
aws auditmanager deregister-account
```

Audit Manager API

Before you start

Before you disable Audit Manager, you can use the [UpdateSettings](#) API operation to set your preferred data retention policy. By default, Audit Manager retains your data. If you want to delete your data, you can use the [DeregistrationPolicy](#) attribute to request the deletion of your data.

To disable Audit Manager (API)

When you're ready to disable Audit Manager, call the [DeregisterAccount](#) operation.

For more information, choose the previous links to read more in the *Audit Manager API Reference*. This includes information about how to use these operations and parameters in one of the language-specific AWS SDKs.

To re-enable Audit Manager after you disable it

Go to the Audit Manager service homepage and follow the steps to set up Audit Manager as a new user. For more information, see [Setting up AWS Audit Manager \(p. 26\)](#).

Tip

- If you chose to delete your data when you disabled Audit Manager, you must wait until your data is deleted before you can re-enable the service. Depending on how much data you have, this can take up to seven days. However, feel free to try re-enabling Audit Manager before then. In many cases, data is deleted in as little as one hour.
- If you chose not to delete your data when you disabled Audit Manager, your existing assessments moved into a dormant state and stopped collecting evidence as a result. To start collecting evidence again for a pre-existing assessment, [edit the assessment](#) and choose **Save** without making any changes.

Assessment settings

Use this tab to review and update your assessment settings.

Topics

- [Default audit owners \(optional\) \(p. 260\)](#)
- [Assessment report destination \(optional\) \(p. 260\)](#)

- [Notifications \(optional\) \(p. 262\)](#)

Default audit owners (optional)

You can specify the default audit owners who have primary access to your assessments in Audit Manager.

You can update this setting using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

Audit Manager console

You can choose from the AWS accounts listed in the table, or use the search bar to look for other AWS accounts.

To update your default audit owners settings (console)

1. From the **Assessment** settings tab, go to the **Default audit owners** section and choose **Edit**.
2. To add a default audit owner, select the check box next to the account name under **Audit owner**.
3. To remove a default audit owner, clear the check box next to the account name under **Audit owner**.
4. When you're done, choose **Save**.

AWS CLI

To update your default audit owner settings (AWS CLI)

Run the [update-settings](#) command and use the `--default-process-owners` parameter to specify an audit owner.

In the following example, replace the `placeholder text` with your own information. Note that `roleType` can only be `PROCESS_OWNER`.

```
aws auditmanager update-settings --default-process-owners  
  roleType=PROCESS_OWNER,roleArn=arn:aws:iam::111122223333:role/Administrator
```

Audit Manager API

To update your default audit owner settings (API)

Call the [UpdateSettings](#) operation and use the `defaultProcessOwners` parameter to specify default audit owners. Note that `roleType` can only be `PROCESS_OWNER`.

For more information about audit owners, see [Audit owners](#) in the *Concepts and terminology* section of this guide.

Assessment report destination (optional)

When you generate an assessment report, Audit Manager publishes the report to the S3 bucket of your choice. This S3 bucket is referred to as an *assessment report destination*. You can choose the Amazon S3 bucket that Audit Manager stores your assessment reports in.

You can update this setting using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

Audit Manager console

To update your assessment report destination settings (console)

1. From the **Assessment** settings tab, go to the **Assessment report destination** section.
2. To use an existing Amazon S3 bucket, select a bucket name from the dropdown menu.
3. To create a new Amazon S3 bucket, choose **Create new bucket**.
4. When you're done, choose **Save**.

AWS CLI

To update your assessment report destination settings (AWS CLI)

Run the [update-settings](#) command and use the `--default-assessment-reports-destination` parameter to specify an S3 bucket.

In the following example, replace the *placeholder text* with your own information:

```
aws auditmanager update-settings --default-assessment-reports-destination
destinationType=S3,destination=s3://doc-example-destination-bucket
```

Audit Manager API

To update your assessment report destination settings (API)

Call the [UpdateSettings](#) operation and use the `defaultAssessmentReportsDestination` parameter to specify an S3 bucket.

For instructions on how to create an S3 bucket, see [Creating a bucket](#) in the *Amazon S3 User Guide*.

Configuration tips for your assessment report destination

To ensure the successful generation of your assessment report, we recommend that you verify the following configurations for your assessment report destination.

Same-Region buckets

We recommend that you use an S3 bucket that's in the same AWS Region as your assessment. When you use a same-Region bucket and assessment, your assessment report can include up to 22,000 evidence items. Conversely, when you use a cross-Region bucket and assessment, only 3,500 evidence items can be included.

AWS Region

The AWS Region of your customer managed key (if you provided one) must match the Region of your assessment and your assessment report destination S3 bucket. For instructions on how to change the KMS key, see [AWS Audit Manager settings, Data encryption](#). For instructions on how to change the S3 bucket, see [AWS Audit Manager settings, Assessment report destination](#). For a list of supported Audit Manager Regions, see [AWS Audit Manager endpoints and quotas](#) in the *Amazon Web Services General Reference*.

S3 bucket encryption

If your assessment report destination has a bucket policy that requires server-side encryption (SSE) using [SSE-KMS](#), then the KMS key used in that bucket policy must match the KMS key that you configured in your Audit Manager data encryption settings. If you haven't configured a KMS key in your Audit Manager settings, and your assessment report destination bucket policy requires SSE, ensure that the bucket policy allows [SSE-S3](#). For instructions on how to configure the KMS key that's used for data encryption, see [Data encryption settings](#).

Cross-account S3 buckets

Using a cross-account S3 bucket as your assessment report destination isn't supported in the Audit Manager console. It's possible to specify a cross-account bucket as your assessment report destination by using the AWS CLI or one of the AWS SDKs, but for simplicity, we recommend that you not do this. If you do choose to use a cross-account S3 bucket as your assessment report destination, consider the following points.

- By default, S3 objects—such as assessment reports—are owned by the AWS account that uploads the object. You can use the [S3 Object Ownership](#) setting to change this default behavior so that any new objects that are written by accounts with the bucket-owner-full-control canned access control list (ACL) automatically become owned by the bucket owner.

Although it's not a requirement, we recommend that you make the following changes to your cross-account bucket settings. Making these changes ensures that the bucket owner has full control of the assessment reports that you publish to their bucket.

- [Set the object ownership of the S3 bucket](#) to *bucket owner preferred*, instead of the default *object writer*
- [Add a bucket policy](#) to ensure that objects uploaded to that bucket have the bucket-owner-full-control ACL
- To allow Audit Manager to publish reports in a cross-account S3 bucket, you must add the following S3 bucket policy to your assessment report destination. Replace the *placeholder text* with your own information. The Principal element in this policy is the user or role that owns the assessment and creates the assessment report. The Resource specifies the cross-account S3 bucket where the report is published.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "Allow cross account assessment report publishing",  
            "Effect": "Allow",  
            "Principal": {  
                "AWS":  
                    "arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"  
            },  
            "Action": [  
                "s3>ListBucket",  
                "s3PutObject",  
                "s3GetObject",  
                "s3GetBucketLocation",  
                "s3PutObjectAcl",  
                "s3DeleteObject"  
            ],  
            "Resource": [  
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",  
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"  
            ]  
        }  
    ]  
}
```

Notifications (optional)

Audit Manager can send notifications to the Amazon SNS topic that you specify in this setting. If you're subscribed to that SNS topic, you receive notifications when you sign in to Audit Manager.

You can update this setting using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

Audit Manager console

To update your notification settings (console)

1. From the **Assessment** settings tab, go to the **Notifications** section.
2. To use an existing SNS topic, select the topic name from the dropdown menu.
3. To create a new SNS topic, choose **Create new topic**.
4. When you're done, choose **Save**.

AWS CLI

To update your notification settings (AWS CLI)

Run the [update-settings](#) command and use the `--sns-topic` parameter to specify an SNS topic.

In the following example, replace the *placeholder text* with your own information:

```
aws auditmanager update-settings --sns-topic arn:aws:sns:us-east-1:111122223333:my-assessment-topic
```

Audit Manager API

To update your notification settings (API)

Call the [UpdateSettings](#) operation and use the `snsTopic` parameter to specify an SNS topic.

Note

You can use either a standard SNS topic or a FIFO (first-in-first-out) SNS topic. Although Audit Manager supports sending notifications to FIFO topics, the order that messages are sent in isn't guaranteed.

If you want to use an Amazon SNS topic that you don't own, configure your AWS Identity and Access Management (IAM) policy for this. More specifically, you must configure it to allow publishing from the Amazon Resource Name (ARN) of the topic. For more information about IAM, see [Identity and access management for AWS Audit Manager](#).

To learn more about the list of actions that invoke notifications in Audit Manager, see [Notifications in AWS Audit Manager \(p. 270\)](#).

For instructions on how to create an Amazon SNS topic, see [Creating an Amazon SNS topic](#) in the *Amazon SNS User Guide*.

Evidence finder settings

Use this tab to review and update your evidence finder settings.

Topics

- [Evidence finder \(optional\) \(p. 263\)](#)
- [Export destination \(optional\) \(p. 267\)](#)

Evidence finder (optional)

We strongly recommend that you enable evidence finder. Enabling this feature is necessary if you want to run search queries on your evidence.

Follow these steps to enable, disable, or check the status of evidence finder.

Enable evidence finder

You must enable evidence finder in each AWS Region where you want to search for evidence. If you're a delegated administrator for Audit Manager, enable evidence finder to search for evidence for all member accounts in your organization.

Required permissions to enable evidence finder

To enable evidence finder, you need permissions to create and manage an event data store in CloudTrail Lake. To use the feature, you need permissions to perform CloudTrail Lake queries. For an example permission policy that you can use, see [Allow full administrator access](#).

If you need help with permissions, contact your AWS administrator. If you're an AWS administrator, you can copy the required permission statement and [attach it to an IAM policy](#).

Requesting to enable evidence finder

You can complete this task using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

Audit Manager console

To request to enable evidence finder (console)

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. From the **Evidence finder** settings tab, go to the **Evidence finder** section.
3. Choose **Required permission policy**, then **View CloudTrail Lake permissions** to view the required evidence finder permissions. If you don't already have these permissions, you can copy this policy statement and [attach it to an IAM policy](#).
4. Choose **Enable**.
5. In the pop-up window, choose **Request to enable**.

AWS CLI

To request to enable evidence finder (AWS CLI)

Run the [update-settings](#) command with the `--evidence-finder-enabled` parameter.

```
aws auditmanager update-settings --evidence-finder-enabled
```

Audit Manager API

To request to enable evidence finder (API)

Call the [UpdateSettings](#) operation and use the `evidenceFinderEnabled` parameter.

For more information, choose the previous links to read more in the *Audit Manager API Reference*. This includes information about how to use this operation and parameter in one of the language-specific AWS SDKs.

Confirm the status of evidence finder

After you submit your request, it takes up to 10 minutes to enable evidence finder and to create an event data store. As soon as the event data store is created, all new evidence is ingested into the event data store moving forward.

When evidence finder is enabled and the event data store is created, we backfill the newly created event data store with up to two years' worth of your past evidence. This process happens automatically and takes up to seven days to complete.

You can check the current status of evidence finder using the Audit Manager console, the AWS CLI, or the Audit Manager API.

Audit Manager console

To see the current status of evidence finder (console)

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the left navigation pane, choose **Settings**.
3. Under **Enable evidence finder – optional**, review the current status.

Each status is defined as follows:

- **Evidence finder isn't enabled** – You haven't successfully enabled evidence finder yet.
- **You have requested to enable evidence finder** – Your request is pending the event data store being created.
- **Evidence finder is enabled** – The event data store was created. You can now use evidence finder.

Depending how much evidence you have, it takes up to seven days to backfill the new event data store with your past evidence data. A blue information panel indicates that the data backfill is in progress. Feel free to start exploring evidence finder in the meantime. However, keep in mind that not all data is available until the backfill is complete.

- **You have requested to disable evidence finder** – Your request is pending the event data store being deleted.
- **Evidence finder has been disabled** – Evidence finder has been permanently disabled and the event data store is deleted.

AWS CLI

To see the current status of evidence finder (AWS CLI)

Run the [get-settings](#) command with the --attribute parameter set to EVIDENCE_FINDER_ENABLEMENT.

```
aws auditmanager get-settings --attribute EVIDENCE_FINDER_ENABLEMENT
```

This returns the following information:

enablementStatus

This attribute shows the current status of evidence finder.

- **ENABLE_IN_PROGRESS** – You requested to enable evidence finder. An event data store is currently being created to support evidence finder queries.
- **ENABLED** – An event data store was created and evidence finder is enabled. We recommend waiting seven days until the event data store is backfilled with your past evidence data. You can use evidence finder in the meantime, but not all data is available until the backfill is complete.
- **DISABLE_IN_PROGRESS** – You requested to disable evidence finder, and your request is pending the event data store being deleted.

- DISABLED – You permanently disabled evidence finder and the event data store is deleted. You can't re-enable evidence finder after this point.

backfillStatus

This attribute shows the current status of the evidence data backfill.

- NOT_STARTED – The backfill hasn't started yet.
- IN_PROGRESS – The backfill is in progress. This takes up to seven days to complete, depending on the amount of evidence data.
- COMPLETED – The backfill is complete. All of your past evidence is now queryable.

Audit Manager API

To see the current status of evidence finder (API)

Call the [GetSettings](#) operation with the attribute parameter set to EVIDENCE_FINDER_ENABLEMENT. This returns the following information:

enablementStatus

This attribute shows the current status of evidence finder.

- ENABLE_IN_PROGRESS - You requested to enable evidence finder. An event data store is currently being created to support evidence finder queries.
- ENABLED - An event data store was created and evidence finder is enabled. We recommend waiting seven days until the event data store is backfilled with your past evidence data. You can use evidence finder in the meantime, but not all data is available until the backfill is complete.
- DISABLE_IN_PROGRESS - You requested to disable evidence finder, and your request is pending the deletion of the event data store.
- DISABLED - You permanently disabled evidence finder and the event data store is deleted. You can't re-enable evidence finder after this point.

backfillStatus

This attribute shows the current status of the evidence data backfill.

- NOT_STARTED means that the backfill hasn't started yet.
- IN_PROGRESS means that the backfill is in progress. This takes up to seven days to complete, depending on the amount of evidence data.
- COMPLETED means that the backfill is complete. All of your past evidence is now queryable.

For more information, see [evidenceFinderEnablement](#) in the *Audit Manager API Reference*.

Disable evidence finder

If you no longer want to use evidence finder, you can disable this feature at any time.

Warning

Disabling evidence finder deletes the CloudTrail Lake event data store that Audit Manager created. As a result, you can't re-enable the feature. To re-use evidence finder after you disable it, you must [disable AWS Audit Manager](#), and then [re-enable](#) the service completely.

Required permissions to disable evidence finder

To disable evidence finder, you need permissions to delete an event data store in CloudTrail Lake. For an example policy that you can use, see [Permissions to disable evidence finder](#).

If you need help with permissions, contact your AWS administrator. If you're an AWS administrator, you can [attach the required permission statement to an IAM policy](#).

Disabling evidence finder

You can complete this task using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

Audit Manager console

To disable evidence finder (console)

1. In the **Evidence finder** section of the Audit Manager settings page, choose **Disable**.
2. In the pop-up window that appears, enter **Yes** to confirm your decision.
3. Choose **Request to disable**.

AWS CLI

To disable evidence finder (AWS CLI)

Run the [update-settings](#) command with the `--no-evidence-finder-enabled` parameter.

```
aws auditmanager update-settings --no-evidence-finder-enabled
```

Audit Manager API

To disable evidence finder (API)

Call the [UpdateSettings](#) operation and use the `evidenceFinderEnabled` parameter.

For more information, choose the previous links to read more in the *Audit Manager API Reference*. This includes information about how to use this operation and parameter in one of the language-specific AWS SDKs.

Export destination (optional)

When you run queries in evidence finder, you can export your search results into a comma-separated values (CSV) file. Use this setting to choose the default S3 bucket where Audit Manager saves your exported files.

You can update this setting using the Audit Manager console, the AWS Command Line Interface (AWS CLI), or the Audit Manager API.

Important

Your S3 bucket must have the required permissions policy to allow CloudTrail to write the export files to it. More specifically, the bucket policy must include an `s3:PutObject` action and the bucket ARN, and list CloudTrail as the service principal. We provide an [example permission policy](#) that you can use. For instructions on how to attach this policy to your S3 bucket, see [Adding a bucket policy by using the Amazon S3 console](#).

For more tips, see [configuration tips for your export destination](#) on this page.

Audit Manager console

To update your export destination settings (console)

1. From the **Evidence finder** settings tab, go to the **Export destination** section.
2. Choose one of the following options:
 - If you want to remove the current S3 bucket, choose **Remove** to clear your settings.
 - If you want to save a default S3 bucket for the first time, proceed to step 3.
3. Specify the S3 bucket that you want to store your exported files in.
 - Choose **Browse S3** to choose from a list of your buckets.
 - Alternatively, you can enter the bucket URI in this format: **s3://bucketname/prefix**

Tip

To keep your destination bucket organized, you can create an optional folder for your CSV exports. To do so, append a slash (/) and a prefix to the value in the **Resource URI** box (for example, `/evidenceFinderCSVExports`). Audit Manager then includes this prefix when it adds the CSV file to the bucket, and Amazon S3 generates the path specified by the prefix. For more information about prefixes in Amazon S3, see [Organizing objects in the Amazon S3 console](#) in the *Amazon Simple Storage Service User Guide*.

4. When you're done, choose **Save**.

For instructions on how to create an S3 bucket, see [Creating a bucket](#) in the *Amazon S3 User Guide*.

AWS CLI

To update your export destination settings (AWS CLI)

Run the [update-settings](#) command and use the `--default-export-destination` parameter to specify an S3 bucket.

In the following example, replace the `placeholder text` with your own information:

```
aws auditmanager update-settings --default-export-destination
destinationType=S3,destination=s3://doc-example-destination-bucket
```

For instructions on how to create an S3 bucket, see [create-bucket](#) in the *AWS CLI Command Reference*.

Audit Manager API

To update your export destination settings (API)

Call the [UpdateSettings](#) operation and use the `defaultExportDestination` parameter to specify an S3 bucket.

For instructions on how to create an S3 bucket, see [CreateBucket](#) in the *Amazon S3 API Reference*.

Configuration tips for your export destination

To ensure a successful file export, we recommend that you verify the following configurations for your export destination.

AWS Region

The AWS Region of your customer managed key (if you provided one) must match the Region of your assessment. For instructions on how to change your KMS key, see [Audit Manager data encryption settings](#).

Cross-account S3 buckets

Using a cross-account S3 bucket as your export destination isn't supported in the Audit Manager console. It's possible to specify a cross-account bucket using the AWS CLI or one of the AWS SDKs, but for simplicity, we recommend that you not do this. If you do choose to use a cross-account S3 bucket as your export destination, consider the following points.

- By default, S3 objects—such as CSV exports—are owned by the AWS account that uploads the object. You can use the [S3 Object Ownership](#) setting to change this default behavior, so that any new objects that are written by accounts with the bucket-owner-full-control canned access control list (ACL) automatically become owned by the bucket owner.

Although it's not a requirement, we recommend that you make the following changes to your cross-account bucket settings. Making these changes ensures that the bucket owner has full control of the exported files that you publish to their bucket.

- [Set the object ownership of the S3 bucket](#) to *bucket owner preferred*, instead of the default *object writer*
- [Add a bucket policy](#) to ensure that objects uploaded to that bucket have the bucket-owner-full-control ACL
- To allow Audit Manager to export files to a cross-account S3 bucket, you must add the following S3 bucket policy to your export destination bucket. Replace the *placeholder text* with your own information. The Principal element in this policy is the user or role that owns the assessment and exports the file. The Resource specifies the cross-account S3 bucket where the file is exported to.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "Allow cross account file exports",  
            "Effect": "Allow",  
            "Principal": {  
                "AWS":  
                    "arn:aws:iam::AssessmentOwnerAccountId: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/*"  
            ]  
        }  
    ]  
}
```

Notifications in AWS Audit Manager

AWS Audit Manager can notify you about user actions through [Amazon Simple Notification Service \(Amazon SNS\)](#).

Audit Manager sends notifications when one of the following events occurs:

- An audit owner delegates a control set for review.
- A delegate submits a reviewed control set back to the audit owner.
- An audit owner completes the review of a control set.

Prerequisites

Before you set up Amazon SNS notifications in Audit Manager, make sure that you complete the following steps.

1. Create a topic in Amazon SNS if you don't have one already. For instructions, see [Creating an Amazon SNS topic](#) in the *Amazon Simple Notification Service Developer Guide*.
2. Subscribe at least one endpoint to the topic. For example, if you want to receive notifications by text message, subscribe an SMS endpoint to the topic. An SMS endpoint is a mobile phone number. To receive notifications by email, subscribe an email endpoint to the topic. An email endpoint is an email address.
For more information, see [Getting Started](#) in the *Amazon Simple Notification Service Developer Guide*.
3. (Optional) If your topic uses AWS Key Management Service (AWS KMS) for server-side encryption (SSE), you must add permissions to the AWS KMS key policy. For an example policy that you can use, see [Permissions for a KMS key that's attached to an SNS topic](#).

Configuring notifications in AWS Audit Manager

Follow these steps to configure your notifications in AWS Audit Manager.

To configure notifications in AWS Audit Manager

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the left navigation pane, choose **Settings**.
3. Under **Notifications - optional**, specify the SNS topic that you want to use to receive notifications.
 - To use an existing topic, select the topic name from the dropdown menu.
 - To create a new topic, choose **Create new topic**. This takes you to the Amazon SNS console where you can create a topic.
4. When you're done, choose **Save**.

Notes

- You can use either a standard SNS topic or a FIFO (first-in-first-out) SNS topic. Audit Manager supports sending notifications to FIFO topics. However, the order that messages are sent in isn't guaranteed.

- If you want to use an Amazon SNS topic that you don't own, you must configure your AWS Identity and Access Management (IAM) policy. More specifically, you must configure your policy to allow publishing from the Amazon Resource Name (ARN) of the topic. For more information, see [Identity and access management for AWS Audit Manager](#).

Troubleshooting

To find answers to common questions and issues, see [Troubleshooting notification issues](#) in the *Troubleshooting* section of this guide.

Troubleshooting in AWS Audit Manager

You can use the following information to troubleshoot issues that you encounter when working with AWS Audit Manager.

If the issues that you encounter are outside the scope of the following information, or if they persist after you've tried to resolve them, contact [AWS Support](#).

Topics

- [Troubleshooting assessment and evidence collection issues \(p. 272\)](#)
- [Troubleshooting assessment report issues \(p. 279\)](#)
- [Troubleshooting control and control set issues \(p. 282\)](#)
- [Troubleshooting dashboard issues \(p. 288\)](#)
- [Troubleshooting delegated administrator and AWS Organizations issues \(p. 289\)](#)
- [Troubleshooting evidence finder issues \(p. 292\)](#)
- [Troubleshooting framework sharing issues \(p. 300\)](#)
- [Troubleshooting notification issues \(p. 303\)](#)
- [Troubleshooting permission and access issues \(p. 304\)](#)

Troubleshooting assessment and evidence collection issues

You can use the information on this page to resolve common assessment and evidence collection issues in Audit Manager.

Topics

- [I created an assessment but I can't see any evidence yet \(p. 273\)](#)
- [My assessment isn't collecting compliance check evidence from AWS Security Hub \(p. 273\)](#)
- [My assessment isn't collecting compliance check evidence from AWS Config \(p. 274\)](#)
- [My assessment isn't collecting user activity evidence from AWS CloudTrail \(p. 276\)](#)
- [My assessment isn't collecting configuration data evidence for an AWS API call \(p. 276\)](#)
- [My assessment isn't collecting evidence from another AWS service \(p. 276\)](#)
- [My evidence is generated at different intervals, and I'm not sure how often it's being collected \(p. 277\)](#)
- [What happens if I remove an in-scope account from my organization? \(p. 277\)](#)
- [I can't edit the services in scope for my assessment \(p. 278\)](#)
- [What's the difference between a service in scope and a data source type? \(p. 278\)](#)
- [My assessment creation failed \(p. 279\)](#)

- [I disabled and then re-enabled Audit Manager, and now my pre-existing assessments are no longer collecting evidence \(p. 279\)](#)

I created an assessment but I can't see any evidence yet

If you can't see any evidence, it's likely that you either didn't wait at least 24 hours after you created the assessment or that there's a configuration error.

We recommend that you check the following:

1. Make sure that 24 hours passed since you created the assessment. Automated evidence becomes available 24 hours after you create the assessment.
2. Make sure that you're using Audit Manager in the same AWS Region as the AWS service that you're expecting to see evidence for.
3. If you expect to see compliance check evidence from AWS Config and AWS Security Hub, make sure that both the AWS Config and Security Hub consoles display results for these checks. The AWS Config and Security Hub results should display in the same AWS Region that you use Audit Manager in.

If you still can't see evidence in your assessment and it's not due to one of these issues, check the other potential causes that are described on this page.

My assessment isn't collecting compliance check evidence from AWS Security Hub

If you don't see compliance check evidence for an AWS Security Hub control, this could be due to one of the following issues.

Missing configuration in AWS Security Hub

This issue can be caused if you missed some configuration steps when you enabled AWS Security Hub.

Make sure that you enabled Security Hub and configured your settings as follows.

Confirming your Security Hub settings for a single AWS account

If you're using a single AWS account, check the following:

- Confirm that you [enabled AWS Config and configured resource recording for your account](#).
- Confirm that you [enabled the PCI DSS security standard for your account](#).
- Confirm that you [turned on the consolidated control findings setting in Security Hub](#).

Confirming your Security Hub settings for an organization

If you're using Organizations, check the following:

- Confirm that you [enabled AWS Config and configured resource recording for your organization](#).
- Confirm that you [enabled the PCI DSS security standard for every member account of the organization](#).
- Confirm that you [turned on the consolidated control findings setting in Security Hub](#).

- Confirm that the [delegated administrator account that you use in Security Hub](#) is the same one that you use in Audit Manager.
- Confirm that you [enabled your organization accounts as Security Hub member accounts](#).

A Security Hub control name was entered incorrectly in your ControlMappingSource

When you use the Audit Manager API to create a custom control, you can specify a Security Hub control as a [data source mapping](#) for evidence collection. To do this, you enter a control ID as the [keywordValue](#).

If you don't see compliance check evidence for a Security Hub control, it could be that the keywordValue was entered incorrectly in your ControlMappingSource. The keywordValue is case sensitive. If you enter it incorrectly, Audit Manager might not recognize that rule. As a result, you might not collect compliance check evidence for that control as expected.

To fix this issue, [update the custom control](#) and revise the keywordValue. The correct format of a Security Hub keyword varies. For accuracy, reference the list of [supported Security Hub control keywords](#).

AuditManagerSecurityHubFindingsReceiver Amazon EventBridge rule is missing

When you enable Audit Manager, a rule named AuditManagerSecurityHubFindingsReceiver is automatically created and enabled in Amazon EventBridge. This rule enables Audit Manager to collect Security Hub findings as evidence.

If this rule isn't listed and enabled in the AWS Region where you use Security Hub, Audit Manager can't collect Security Hub findings for that Region.

To resolve this issue, go to the [EventBridge console](#) and confirm that the AuditManagerSecurityHubFindingsReceiver rule exists in your AWS account. If the rule doesn't exist, we recommend that you [disable Audit Manager](#) and then re-enable the service. If this action doesn't resolve the issue, or if disabling Audit Manager isn't an option, [contact AWS Support](#) for assistance.

Service-linked AWS Config rules created by Security Hub

Keep in mind that Audit Manager doesn't collect evidence from the [service-linked AWS Config rules that Security Hub creates](#). This is a specific type of managed AWS Config rule that's enabled and controlled by the Security Hub service. Security Hub creates instances of these service-linked rules in your AWS environment, even if other instances of the same rules already exist. As a result, to prevent evidence duplication, Audit Manager doesn't support evidence collection from the service-linked rules.

My assessment isn't collecting compliance check evidence from AWS Config

If you don't see compliance check evidence for an AWS Config rule, this could be due to one of the following issues.

The rule identifier was entered incorrectly in your ControlMappingSource

When you use the Audit Manager API to create a custom control, you can specify an AWS Config rule as a [data source mapping](#) for evidence collection. The [keywordValue](#) that you specify depends on the type of rule.

If you don't see compliance check evidence for an AWS Config rule, it could be that the keywordValue was entered incorrectly in your ControlMappingSource. The keywordValue is

case sensitive. If you enter it incorrectly, Audit Manager might not recognize the rule. As a result, you might not collect compliance check evidence for that rule as intended.

To fix this issue, [update the custom control](#) and revise the keywordValue.

- For custom rules, make sure that the keywordValue has the Custom_ prefix followed by the custom rule name. The format of the custom rule name may vary. For accuracy, visit the [AWS Config console](#) to verify your custom rule names.
- For managed rules, make sure that the keywordValue is the rule identifier in ALL_CAPS_WITH_UNDERSCORES. For example, CLOUDWATCH_LOG_GROUP_ENCRYPTED. For accuracy, reference the list of [supported managed rule keywords](#).

Note

For some managed rules, the rule identifier is different from the rule name. For example, the rule identifier for [restricted-ssh](#) is INCOMING_SSH_DISABLED. Make sure to use the rule identifier, not the rule name. To find a rule identifier, choose a rule from the [list of managed rules](#) and look for its **Identifier** value.

The rule is a service-linked AWS Config rule

You can use [managed rules](#) and [custom rules](#) as a data source mapping for evidence collection. However, Audit Manager doesn't collect evidence from most [service-linked rules](#).

There are only two types of service-linked rule that Audit Manager collects evidence from:

- Service-linked rules from Conformance Packs
- Service-linked rules from AWS Organizations

Audit Manager doesn't collect evidence from other service-linked rules, specifically any rules with an Amazon Resource Name (ARN) that contains the following prefix: arn:aws:config:*:*:config-rule/aws-service-rule/...

The reason that Audit Manager doesn't collect evidence from most service-linked AWS Config rules is to prevent duplicate evidence in your assessments. A service-linked rule is a specific type of managed rule that enables other AWS services to create AWS Config rules in your account. For example, [some Security Hub controls use an AWS Config service-linked rule to run security checks](#). For each Security Hub control that uses a service-linked AWS Config rule, Security Hub creates an instance of the required AWS Config rule in your AWS environment. This happens even if the original rule already exists in your account. Therefore, to avoid collecting the same evidence from the same rule twice, Audit Manager ignores the service-linked rule and doesn't collect evidence from it.

AWS Config isn't enabled and included as a service in scope

AWS Config must be enabled in your AWS account. It must also be included as a service in scope for your assessment. After you've set up AWS Config in this way, Audit Manager collects evidence each time the evaluation of an AWS Config rule occurs.

First, make sure that you enabled AWS Config in your AWS account. For instructions, see [Enable and set up AWS Config](#).

Next, make sure that you included AWS Config as a service in scope for your assessment. To review the current services in scope for your assessment, see [Review an assessment, AWS services tab](#). To edit the list of services in scope for an assessment, see [Edit AWS services in scope](#).

The AWS Config rule evaluated a resource configuration before you set up your assessment

If your AWS Config rule is set up to evaluate configuration changes for a specific resource, you might see a mismatch between the evaluation in AWS Config and the evidence in Audit Manager. This happens if the rule evaluation occurred before you set up the control in your Audit Manager assessment. In this case, Audit Manager doesn't generate evidence until the underlying resource changes state again and triggers a re-evaluation of the rule.

As a workaround, you can navigate to the rule in the AWS Config console and [manually re-evaluate the rule](#). This invokes a new evaluation of all of the resources that pertain to that rule.

My assessment isn't collecting user activity evidence from AWS CloudTrail

When you use the Audit Manager API to create a custom control, you can specify a CloudTrail event name as a [data source mapping](#) for evidence collection. To do so, you enter the event name as the [keywordValue](#).

If you don't see user activity evidence for a CloudTrail event, it could be that the [keywordValue](#) was entered incorrectly in your [ControlMappingSource](#). The [keywordValue](#) is case sensitive. If you enter it incorrectly, Audit Manager might not recognize the event name. As a result, you might not collect user activity evidence for that event as intended.

To fix this issue, [update the custom control](#) and revise the [keywordValue](#). Make sure that the event is written as `serviceprefix_ActionName`. For example, `cloudtrail_StartLogging`. For accuracy, review the AWS service prefix and action names in the [Service Authorization Reference](#).

My assessment isn't collecting configuration data evidence for an AWS API call

When you use the Audit Manager API to create a custom control, you can specify an AWS API call as a [data source mapping](#) for evidence collection. To do so, you enter the API call as the [keywordValue](#).

If you don't see configuration data evidence for an AWS API call, it could be that the [keywordValue](#) was entered incorrectly in your [ControlMappingSource](#). The [keywordValue](#) is case sensitive. If you enter it incorrectly, Audit Manager might not recognize the API call. As a result, you might not collect configuration data evidence for that API call as intended.

To fix this issue, [update the custom control](#) and revise the [keywordValue](#). Make sure that the API call is written as `serviceprefix_ActionName`. For example, `iam_ListGroups`. For accuracy, reference the list of [supported API calls](#).

My assessment isn't collecting evidence from another AWS service

If an AWS service isn't selected as in scope for your assessment, Audit Manager doesn't collect evidence from resources related to that service. This is also the case if an AWS service is selected but you haven't enabled it in your environment.

If you created your assessment from a custom framework, you can [edit the services in scope for your assessment](#). You can then specify additional AWS services that you want to collect evidence from. After you add these services, evidence becomes available after 24 hours.

Note

If you created your assessment from a standard framework, the list of AWS services in scope is preselected and can't be edited. This is because when you create an assessment from a standard framework, Audit Manager automatically maps and selects the relevant data sources and services for you. The selection is made based on the requirements of the standard framework. Note that, for standard frameworks that contain manual controls only, no AWS services are in scope.

The workaround for editing the AWS services in scope while still creating an assessment based on a standard framework is to [customize the standard framework](#). By using this workaround,

you can use the framework that you customized to [create a new assessment](#). In this assessment, you can then specify which AWS services are in scope.

My evidence is generated at different intervals, and I'm not sure how often it's being collected

The controls in Audit Manager assessments are mapped to various data sources. Each data source has a different evidence collection frequency. As a result, there's no one-size-fits-all answer for how often evidence is collected. Some data sources evaluate compliance, whereas others only capture resource state and change data without a compliance determination.

The following is a summary of the different data source types and how often they collect evidence.

Data source type	Description	Evidence collection frequency	When this control is active in an assessment
AWS CloudTrail	Tracks a specific user activity.	Continual	Audit Manager filters your CloudTrail logs based on the keyword that you choose. The processed logs are imported as User activity evidence.
AWS Security Hub	Captures a snapshot of your resource security posture by reporting findings from Security Hub.	Based on the schedule of the Security Hub check (typically around every 12 hours)	Audit Manager retrieves the security finding directly from Security Hub. The finding is imported as Compliance check evidence.
AWS Config	Captures a snapshot of your resource security posture by reporting findings from AWS Config.	Based on the settings that are defined in the AWS Config rule	Audit Manager retrieves the rule evaluation directly from AWS Config. The evaluation is imported as Compliance check evidence.
AWS API calls	Takes a snapshot of your resource configuration directly through an API call to the specified AWS service.	Daily, weekly, or monthly	Audit Manager makes the API call based on the frequency that you specify. The response is imported as Configuration data evidence.

Regardless of the evidence collection frequency, new evidence is collected automatically for as long as the assessment is active. For more information, see [Evidence collection frequency](#).

To learn more, see [Supported control data sources for automated evidence](#) and [Changing the evidence collection frequency for a control](#).

What happens if I remove an in-scope account from my organization?

When an in-scope account is removed from your organization, Audit Manager no longer collects evidence for that account. However, the account continues to show in your assessment under the **AWS accounts**

tab. To remove the account from the list of accounts in scope, [edit the assessment](#). The removed account no longer shows in the list during editing, and you can save your changes without that account in scope.

I can't edit the services in scope for my assessment

When you use the Audit Manager console to create an assessment from a standard framework, the list of AWS services in scope is selected by default. This list can't be edited. This is because Audit Manager automatically maps and selects the data sources and services for you. This selection is made according to the requirements of the standard framework. If the standard framework that you selected contains only manual controls, no AWS services are in scope for your assessment, and you can't add any services to your assessment.

If you need to edit the list of services in scope, use the [UpdateAssessment](#) API operation that's provided by Audit Manager. Alternatively, you can [customize the standard framework](#) and then create an assessment from the custom framework.

What's the difference between a service in scope and a data source type?

A [service in scope](#) is an AWS service that's specified as part of your assessment. When a service is in scope, Audit Manager collects evidence about your usage of that service and its resources.

A [data source type](#) indicates where exactly the evidence is collected from. If you upload your own evidence, the data source type is *Manual*. If Audit Manager collects the evidence, the data source can be one of four types.

1. AWS Security Hub – Captures a snapshot of your resource security posture by reporting findings from Security Hub.
2. AWS Config – Captures a snapshot of your resource security posture by reporting findings from AWS Config.
3. AWS CloudTrail – Tracks a specific user activity for a resource.
4. AWS API calls – Takes a snapshot of your resource configuration directly through an API call to a specific AWS service.

Here are two examples to illustrate the difference between a service in scope and a data source type.

Example 1

Let's say that you want to collect evidence for a control that's named *4.1.2 - Disallow public write access to S3 buckets*. This control checks the access levels of your S3 bucket policies. For this control, Audit Manager uses a specific AWS Config rule ([s3-bucket-public-write-prohibited](#)) to look for an evaluation of your S3 buckets. In this example, the following is true:

- The [service in scope](#) is Amazon S3
- The [resources](#) that are being assessed are your S3 buckets
- The [data source type](#) is AWS Config
- The [data source mapping](#) is a specific AWS Config rule ([s3-bucket-public-write-prohibited](#))

Example 2

Let's say that you want to collect evidence for a HIPAA control that's named *164.308(a)(5)(ii)(C)*. This control requires a monitoring procedure for detecting inappropriate sign-ins. For this control, Audit

Manager uses CloudTrail logs to look for all [AWS Management Console sign-in events](#). In this example, the following is true:

- The [service in scope](#) is IAM
- The [resources](#) that are being assessed are your users
- The [data source type](#) is CloudTrail
- The [data source mapping](#) is a specific CloudTrail event (ConsoleLogin)

My assessment creation failed

If your assessment creation fails, it could be because you selected too many AWS accounts in your assessment scope. If you're using AWS Organizations, Audit Manager can support up to approximately 150 member accounts in the scope of a single assessment. If you exceed this number, the assessment creation might fail. As a workaround, you can run multiple assessments with different accounts in scope for each assessment.

I disabled and then re-enabled Audit Manager, and now my pre-existing assessments are no longer collecting evidence

When you disable Audit Manager and choose not to delete your data, your existing assessments move into a dormant state and stop collecting evidence. This means that when you re-enable Audit Manager, the assessments that you previously created remain available. However, they don't automatically resume evidence collection.

To start collecting evidence again for a pre-existing assessment, [edit the assessment](#) and choose **Save** without making any changes.

Troubleshooting assessment report issues

You can use the information on this page to resolve common assessment report issues in Audit Manager.

Topics

- [My assessment report failed to generate \(p. 279\)](#)
- [I followed the checklist above, and my assessment report still failed to generate \(p. 280\)](#)
- [I get an access denied error when I try to generate a report \(p. 281\)](#)
- [I'm unable to unzip the assessment report \(p. 281\)](#)
- [When I choose an evidence name in a report, I'm not redirected to the evidence details \(p. 281\)](#)
- [My assessment report generation is stuck in In progress status, and I'm not sure how this impacts my billing \(p. 282\)](#)
- [See also \(p. 282\)](#)

My assessment report failed to generate

Your assessment report might have failed to generate for a number of reasons. You can start to troubleshoot this issue by checking the most frequent causes. Use the following checklist to get started.

1. Check if any of your AWS Region information doesn't match up:

- a. **Does the AWS Region of your customer managed key match the AWS Region of your assessment?**

If you provided your own KMS key for Audit Manager data encryption, the key must be in the same AWS Region as your assessment. To resolve this issue, change the KMS key to one that's in the same Region as your assessment. For instructions on how to change the KMS key, see [AWS Audit Manager settings, Data encryption](#).

- b. **Does the AWS Region of your customer managed key match the AWS Region of your S3 bucket?**

If you provided your own KMS key for Audit Manager data encryption, the key must be in the same AWS Region as the S3 bucket that you use as your assessment report destination. To resolve this issue, you can change either the KMS key or the S3 bucket so that they're both in the same Region as your assessment. For instructions on how to change the KMS key, see [AWS Audit Manager settings, Data encryption](#). For instructions on how to change the S3 bucket, see [AWS Audit Manager settings, Assessment report destination](#).

2. Check the permissions of the S3 bucket that you're using as the assessment report destination:

- a. **Does the IAM entity that's generating the assessment report have the necessary permissions for the S3 bucket?**

The IAM entity must have the required S3 bucket permissions to publish reports in that bucket. We provide an [example policy](#) that you can use. For instructions on how to specify a different S3 bucket, see [AWS Audit Manager settings, Assessment report destination](#).

- b. **Does the S3 bucket have a bucket policy that requires server-side encryption (SSE) using SSE-KMS?**

If yes, the KMS key that's used in that bucket policy must match the KMS key that's specified in your Audit Manager data encryption settings. If you didn't configure a KMS key in your Audit Manager settings, and your S3 bucket policy requires SSE, ensure that the bucket policy allows [SSE-S3](#). For instructions on how to change the KMS key, see [AWS Audit Manager settings, Data encryption](#). For instructions on how to change the S3 bucket, see [AWS Audit Manager settings, Assessment report destination](#).

If you're still unable to successfully generate an assessment report, review the following issues on this page.

I followed the checklist above, and my assessment report still failed to generate

Audit Manager limits how much evidence you can add to an assessment report. The limit is based on the AWS Region of your assessment, the Region of the S3 bucket that's used as your assessment report destination, and whether your assessment uses a customer managed AWS KMS key.

1. The limit is 22,000 for same-Region reports (where the S3 bucket and assessment are in the same AWS Region)
2. The limit is 3,500 for cross-Region reports (where the S3 bucket and assessment are in different AWS Regions)
3. The limit is 3,500 if the assessment uses a customer managed KMS key

If you try to generate a report that contains more evidence than this, the operation might fail.

As a workaround, you can generate multiple assessment reports rather than one larger assessment report. By doing this, you can export evidence from your assessment into more manageable-sized batches.

I get an *access denied* error when I try to generate a report

You will get an *access denied* error if your assessment was created by a delegated administrator account that the KMS key that's specified in your Audit Manager settings doesn't belong to. To avoid this error, when you designate a delegated administrator for Audit Manager, make sure that the delegated administrator account has access on the KMS key that you provided when setting up Audit Manager.

You might also receive an *access denied* error if you don't have write permissions for the S3 bucket that you're using as your assessment report destination.

If you get an *access denied* error, make sure that you meet the following requirements:

- Your KMS key in your Audit Manager settings gives permissions to the delegated administrator. You can configure this by following the instructions in [Allowing users in other accounts to use a KMS key](#) in the *AWS Key Management Service Developer Guide*. For instructions on how to review and change your encryption settings in Audit Manager, see [Data encryption](#).
- You have a permissions policy that grants you write access for the S3 bucket that you're using as the assessment report destination. More specifically, your permissions policy contains an s3:PutObject action, specifies the ARN of the S3 bucket, and includes the KMS key that's used to encrypt your assessment reports. For an example policy that you can use, see [Identity-based policy examples for AWS Audit Manager](#).

Note

If you change your Audit Manager data encryption settings, these changes apply to the new assessments that you create moving forward. This includes any assessment reports that you create from your new assessments.

The changes don't apply to existing assessments that you created before you changed your encryption settings. This includes new assessment reports that you create from existing assessments, in addition to existing assessment reports. Existing assessments—and all their assessment reports—continue to use the old KMS key. If the IAM identity that's generating the assessment report doesn't have permissions to use the old KMS key, you can grant permissions at the key policy level.

I'm unable to unzip the assessment report

If you can't unzip the assessment report on Windows, it's likely that Windows Explorer can't extract it because its file path has several nested folders or long names. This is because, under the Windows file naming system, the folder path, file name, and file extension can't exceed 259 characters. Otherwise, this results in a Destination Path Too Long error.

To resolve this issue, try moving the zip file to the parent folder of its current location. You can then try again to unzip it from there. Alternatively, you can also try shortening the name of the zip file or extracting it to a different location that has a shorter file path.

When I choose an evidence name in a report, I'm not redirected to the evidence details

This issue might happen if you're interacting with the assessment report in a browser, or using the default PDF reader that's installed on your operating system. Some browser and system default PDF readers don't allow the opening of relative links. This means that, although hyperlinks might work within the assessment report summary PDF (such as hyperlinked control names in the table of contents),

hyperlinks are ignored when you attempt to navigate away from the assessment summary PDF to a separate evidence detail PDF.

If you encounter this issue, we recommend that you use a dedicated PDF reader to interact with your assessment reports. For a reliable experience, we recommend that you install and use Adobe Acrobat Reader, which you can download at the [Adobe website](#). Other PDF readers are also available, but Adobe Acrobat Reader has been proven to work consistently and reliably with Audit Manager assessment reports.

My assessment report generation is stuck in *In progress* status, and I'm not sure how this impacts my billing

Assessment report generation has no impact on billing. You're only billed based on the evidence that your assessments collect. For more information about pricing, see [AWS Audit Manager Pricing](#).

See also

The following pages contain troubleshooting guidance about generating an assessment report from evidence finder:

- [I can't generate multiple assessment reports from my search results](#)
- [I can't add individual search results to an assessment report](#)
- [Not all of my evidence finder results are included in the assessment report](#)
- [I want to generate an assessment report from my search results, but my query statement is failing](#)

Troubleshooting control and control set issues

You can use the information on this page to resolve common issues with controls in Audit Manager.

General issues

- [I can't see any controls or control sets in my assessment \(p. 283\)](#)
- [I can't upload manual evidence to a control \(p. 283\)](#)

AWS Config integration issues

- [I need to use multiple AWS Config rules as a data source for a single control \(p. 283\)](#)
- [The custom rule option is unavailable when I'm configuring a control data source \(p. 283\)](#)
- [The custom rule option is available, but no rules appear in the dropdown list \(p. 283\)](#)
- [Some custom rules are available, but I can't see the rule that I want to use \(p. 284\)](#)
- [I can't see the managed rule that I want to use \(p. 285\)](#)
- [I want to share a custom framework, but it has controls that use custom AWS Config rules as a data source. Can the recipient collect evidence for these controls? \(p. 287\)](#)
- [What happens when a custom rule is updated in AWS Config? Do I need to take any action in Audit Manager? \(p. 287\)](#)

I can't see any controls or control sets in my assessment

In short, to view the controls for an assessment, you must be specified as an audit owner for that assessment. Moreover, you need the necessary IAM permissions to view and manage the related Audit Manager resources.

If you need access to the controls in an assessment, ask one of the audit owners for that assessment to specify you as audit owner. You can specify audit owners when you're [creating](#) or [editing](#) an assessment.

Make sure also that you have the necessary permissions to manage the assessment. We recommend that audit owners use the [AWSAuditManagerAdministratorAccess](#) policy. If you need help with IAM permissions, contact your administrator or [AWS Support](#). For more information about how to attach a policy to an IAM identity, see [Adding Permissions to a User](#) and [Adding and removing IAM identity permissions](#) in the *IAM User Guide*.

I can't upload manual evidence to a control

If you can't manually upload evidence to a control, it's likely because the control is in *inactive* status.

To upload manual evidence to a control, you must first change the control status to either *Under review* or *Reviewed*. For more information, see [Update control status](#).

Important

Each AWS account can only manually upload up to 100 evidence files to a control each day. Exceeding this daily quota causes any additional manual uploads to fail for that control. If you need to upload a large amount of manual evidence to a single control, upload your evidence in batches across several days.

I need to use multiple AWS Config rules as a data source for a single control

You can use a combination of managed rules and custom rules for a single control. To do this, set up multiple data sources for the control, and select your preferred rule type for each one. You can define up to 10 data sources for a single custom control.

The custom rule option is unavailable when I'm configuring a control data source

This means that you don't have permissions to view custom rules for your AWS account or organization. More specifically, you don't have permissions to perform the [DescribeConfigRules](#) operation in the Audit Manager console.

To resolve this issue, contact your AWS administrator for help. If you're an AWS administrator, you can provide permissions for your users or groups by [managing your IAM policies](#).

The custom rule option is available, but no rules appear in the dropdown list

This means that no custom rules are enabled and available for use in your AWS account or organization.

If you don't have any custom rules yet in AWS Config, you can create one. For instructions, see [AWS Config custom rules](#) in the *AWS Config Developer Guide*.

If you're expecting to see a custom rule, check the following troubleshooting item.

Some custom rules are available, but I can't see the rule that I want to use

If you can't see the custom rule that you're expecting to find, this could be due to one of the following issues.

Your account is excluded from the rule

It's possible that the delegated administrator account that you're using is excluded from the rule.

Your organization's management account (or one of the AWS Config delegated administrator accounts) can create custom organization rules using the AWS Command Line Interface (AWS CLI). When they do so, they can specify a [list of accounts to be excluded](#) from the rule. If your account is on this list, the rule isn't available in Audit Manager.

To resolve this issue, contact your AWS Config administrator for help. If you're an AWS Config administrator, you can update the list of excluded accounts by running the [put-organization-config-rule](#) command.

The rule wasn't successfully created and enabled in AWS Config

It's also possible that the custom rule wasn't created and enabled successfully. If an [error occurred when creating the rule](#), or the rule isn't [enabled](#), it doesn't appear in the list of available rules in Audit Manager.

For assistance with this issue, we recommend that you contact your AWS Config administrator.

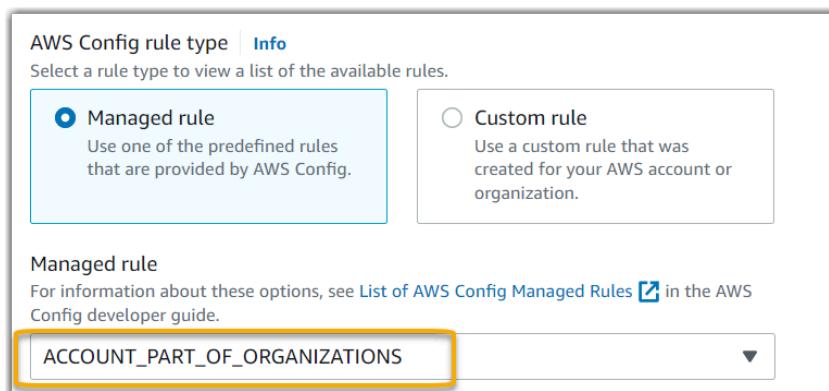
The rule is a managed rule

If you can't find the rule that you're looking for under the dropdown list of custom rules, it's possible that the rule is a managed rule.

You can use the [AWS Config console](#) to verify if a rule is a managed rule. To do so, choose **Rules** in the left navigation menu and look for the rule in the table. If the rule is a managed rule, the **Type** column shows **AWS managed**.

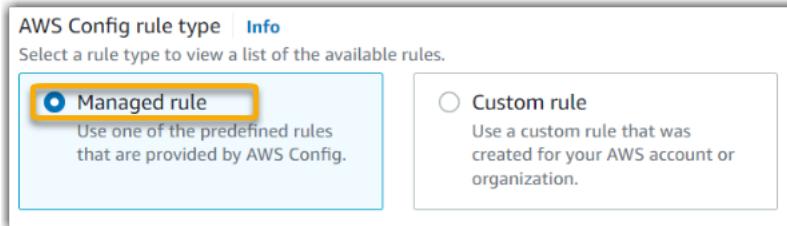
Name	Remediation action	Type	Compliance
account-part-of-organizations	Not set	AWS managed	Compliant

After you've confirmed that it's a managed rule, return to Audit Manager and select **Managed rule** as the rule type. Then, look for the managed rule identifier keyword in the dropdown list of managed rules.



I can't see the managed rule that I want to use

Before you select a rule from the dropdown list in the Audit Manager console, make sure that you selected **Managed rule** as the rule type.



If you still can't see the managed rule that you're expecting to find, it's possible that you're looking for the rule *name*. Instead, you must look for the rule *identifier*.

If you're using a default managed rule, the name and the identifier are similar. The name is in lowercase and uses dashes (for example, `iam-policy-in-use`). The identifier is in uppercase and uses underscores (for example, `IAM_POLICY_IN_USE`). To find the identifier for a default managed rule, review the [list of supported AWS Config managed rule keywords](#) and follow the link for the rule that you want to use. This takes you to the AWS Config documentation for that managed rule. From here, you can see both the name and the identifier. Look for the identifier keyword in the Audit Manager dropdown list.

The screenshot shows the AWS Config documentation page for the `iam-policy-in-use` rule. The rule name is highlighted with a yellow box. Key details shown include:

- Identifier:** `IAM_POLICY_IN_USE`
- Trigger type:** Periodic
- AWS Region:** All supported AWS regions except Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Osaka), Europe (Milan) Region

If you're using a customized managed rule, you can use the [AWS Config console](#) to find the rule identifier. For example, let's say that you want to use the managed rule called `customized-iam-policy-in-use`. To find the identifier for this rule, go to the AWS Config console, choose **Rules** in the left navigation menu, and choose the rule in the table.

Rules			
		View details	Edit rule
		Any status	Add rule
Name	Remediation action	Type	
<code>customized-iam-policy-in-use</code>	Not set	AWS managed	

Choose **Edit** to open details about the managed rule.

The screenshot shows a card for a managed rule named "customized-iam-policy-in-use". At the top right is an "Actions" dropdown menu with an "Edit" button highlighted by a yellow box. Below the title, there's a section titled "Rule details" with three columns: "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), and "Last successful evaluation" (Not available).

Under the **Details** section, you can find the source identifier that the managed rule was created from (IAM_POLICY_IN_USE).

The screenshot shows the "Edit rule" dialog box with the "Details" tab selected. It includes fields for "Name" (customized-iam-policy-in-use) and "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.). Below these, the "Managed rule name" field contains "IAM_POLICY_IN_USE", which is highlighted with a yellow box.

You can now return to the Audit Manager console and select the same identifier keyword from the dropdown list.

The screenshot shows the "AWS Config rule type" selection screen. It has two options: "Managed rule" (selected) and "Custom rule". Below the options, a dropdown menu shows "IAM_POLICY_IN_USE" selected, which is highlighted with a yellow box. A link to the "List of AWS Config Managed Rules" is also present.

I want to share a custom framework, but it has controls that use custom AWS Config rules as a data source. Can the recipient collect evidence for these controls?

Yes, the recipient can collect evidence for these controls, but a few steps are needed to achieve this.

For Audit Manager to collect evidence using an AWS Config rule as a data source mapping, the following must be true. This applies to both managed rules and custom rules.

1. The rule must exist in the recipient's AWS environment
2. The rule must be enabled in the recipient's AWS environment

Remember that the custom AWS Config rules in your account likely don't exist already in the recipient's AWS environment. Moreover, when the recipient accepts the share request, Audit Manager doesn't recreate any of your custom rules in their account. For the recipient to collect evidence using your custom rules as a data source mapping, they must create the same custom rules in their instance of AWS Config. After the recipient [creates](#) and then [enables](#) the rules, Audit Manager can collect evidence from that data source.

We recommend that you communicate with the recipient to let them know if any custom rules need to be created in their instance of AWS Config.

What happens when a custom rule is updated in AWS Config? Do I need to take any action in Audit Manager?

For rule updates within your AWS environment

If you update a custom rule within your AWS environment, no action is needed in Audit Manager. Audit Manager detects and handles the rule updates as described in the following table. Audit Manager doesn't notify you when a rule update is detected.

Scenario	What Audit Manager does	What you need to do
A custom rule is updated in your instance of AWS Config.	Audit Manager continues to report findings for that rule using the updated rule definition.	No action is needed.
A custom rule is deleted in your instance of AWS Config.	Audit Manager stops reporting findings for the deleted rule.	No action is needed. If you want to, you can edit the custom controls that used the deleted rule as a data source mapping. Doing so helps to clean up your data source settings by removing the deleted rule. Otherwise, the deleted rule name remains as an unused data source mapping.

For rule updates outside your AWS environment

If a custom rule is updated outside of your AWS environment, Audit Manager doesn't detect the rule update. This is something to consider if you use shared custom frameworks. This is because, in this scenario, the sender and the recipient each work in separate AWS environments. The following table provides recommended actions for this scenario.

Your role	Scenario	Recommended action
Sender	<ul style="list-style-type: none">You shared a framework that uses custom rules as a data source mapping.After you shared the framework, you updated or deleted one of those rules in AWS Config.	Let the recipient know about your update. That way, they can apply the same update and stay in sync with the latest rule definition.
Recipient	<ul style="list-style-type: none">You accepted a shared framework that uses custom rules as a data source mapping.After you recreated the custom rules in your instance of AWS Config, the sender updated or deleted one of those rules.	Make the corresponding rule update in your own instance of AWS Config.

Troubleshooting dashboard issues

You can use the information on this page to resolve common dashboard issues in Audit Manager.

Topics

- [There isn't any data on my dashboard \(p. 288\)](#)
- [The CSV download option isn't available \(p. 288\)](#)
- [I don't see the downloaded file when trying to download a CSV file \(p. 289\)](#)
- [A specific control or control domain is missing from the dashboard \(p. 289\)](#)
- [The daily snapshot shows varying amounts of evidence each day. Is this normal? \(p. 289\)](#)

There isn't any data on my dashboard

If the numbers in the [daily snapshot widget](#) display a hyphen (-), this indicates that no data is available. You must have at least one active assessment to see data in the dashboard. To get started, [create an assessment](#). After a 24-hour period, your assessment data will start to appear in the dashboard.

Note

If the numbers in the [daily snapshot widget](#) display a zero (0), this indicates that your active assessments (or your selected assessment) have no non-compliant evidence.

The CSV download option isn't available

This option is available for individual assessments only. Make sure that you applied an [the section called "Assessment filter" \(p. 46\)](#) to the dashboard, then try again. Keep in mind that you can only download one CSV file at a time.

I don't see the downloaded file when trying to download a CSV file

If a control domain contains a large number of controls, there might be a short delay while Audit Manager generates the CSV file. After the file is generated, it downloads automatically.

If you still don't see the downloaded file, make sure that your internet connection is working normally and you're using the most current version of your web browser. In addition, check your recent downloads folder. Files download into the default location that's determined by your browser. If this doesn't resolve your issue, try downloading the file using a different browser.

A specific control or control domain is missing from the dashboard

This likely means that your active assessments (or specified assessment) don't have any relevant data for that control or control domain.

A control domain is displayed on the dashboard only if both of the following two criteria are met:

- Your active assessments (or specified assessment) contain at least one control that's related to that domain
- At least one control within that domain collected evidence on the date at the top of the dashboard

A control is displayed within a domain only if it collected evidence on the date at the top of the dashboard.

The daily snapshot shows varying amounts of evidence each day. Is this normal?

Not all evidence is collected on a daily basis. The controls in Audit Manager assessments are mapped to different data sources, and each one can have a different evidence collection schedule. As a result, it's expected that the daily snapshot displays a varying amount of evidence each day. For more information about evidence collection frequency, see [How AWS Audit Manager collects evidence](#).

Troubleshooting delegated administrator and AWS Organizations issues

You can use the information on this page to resolve common delegated administrator issues in Audit Manager.

Topics

- [I can't set up Audit Manager with my delegated administrator account \(p. 290\)](#)
- [When I create an assessment, I can't see the accounts from my organization under Accounts in scope \(p. 290\)](#)
- [I get an access denied error when I try to generate an assessment report using my delegated administrator account \(p. 290\)](#)
- [What happens in Audit Manager if I unlink a member account from my organization? \(p. 291\)](#)
- [What happens if I relink a member account to my organization? \(p. 291\)](#)

- [What happens if I migrate a member account from one organization to another? \(p. 291\)](#)

I can't set up Audit Manager with my delegated administrator account

Although multiple delegated administrators are supported in AWS Organizations, Audit Manager allows only one delegated administrator. If you attempt to designate multiple delegated administrators in Audit Manager, you receive the following error message:

- Console: 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 111111111111 from 222222222222 to 333333333333

Choose the one individual account that you want to use as your delegated administrator in Audit Manager. Make sure that you register the delegated administrator account in Organizations first, and then [add the same account as a delegated administrator](#) in Audit Manager.

When I create an assessment, I can't see the accounts from my organization under *Accounts in scope*

If you want your Audit Manager assessment to include multiple accounts from your organization, you must specify a delegated administrator.

Make sure that you configured a delegated administrator account for Audit Manager. For instructions, see [Settings, Delegated administrator](#).

Some issues to keep in mind:

- You can't use your AWS Organizations management account as a delegated administrator in Audit Manager.
- If you want to enable Audit Manager in more than one AWS Region, you must designate a delegated administrator account separately in each Region. In your Audit Manager settings, designate the same delegated administrator account across all Regions.
- When you designate a delegated administrator, make sure that the delegated administrator account has access on the KMS key that you provide when setting up Audit Manager. To learn how to review and change your encryption settings, see [Data encryption](#).

I get an *access denied* error when I try to generate an assessment report using my delegated administrator account

You will get an *access denied* error if your assessment was created by a delegated administrator account that the KMS key that's specified in your Audit Manager settings doesn't belong to. To avoid this error, when you designate a delegated administrator for Audit Manager, make sure that the delegated administrator account has access on the KMS key that you provided when setting up Audit Manager.

You might also receive an *access denied* error if you don't have write permissions for the S3 bucket that you're using as your assessment report destination.

If you get an access denied error, make sure that you meet the following requirements:

- Your KMS key in your Audit Manager settings gives permissions to the delegated administrator. You can configure this by following the instructions in [Allowing users in other accounts to use a KMS key](#) in the *AWS Key Management Service Developer Guide*. For instructions on how to review and change your encryption settings in Audit Manager, see [Data encryption](#).
- You have a permissions policy that grants you write access for the assessment report destination. More specifically, your permissions policy contains an s3:PutObject action, specifies the ARN of the S3 bucket, and includes the KMS key that's used to encrypt your assessment reports. For an example policy that you can use, see [Identity-based policy examples for AWS Audit Manager](#).

Note

If you change your Audit Manager data encryption settings, these changes apply to the new assessments that you create moving forward. This includes any assessment reports that you create from your new assessments.

The changes don't apply to existing assessments that you created before you changed your encryption settings. This includes new assessment reports that you create from existing assessments, in addition to existing assessment reports. Existing assessments—and all their assessment reports—continue to use the old KMS key. If the IAM identity that's generating the assessment report doesn't have permissions to use the old KMS key, you can grant permissions at the key policy level.

What happens in Audit Manager if I unlink a member account from my organization?

When you unlink a member account from an organization, Audit Manager receives a notification about this event. Audit Manager then automatically removes that AWS account from the *accounts in scope* lists of your existing assessments. When you specify the scope of new assessments moving forward, the unlinked account no longer appears in the list of eligible AWS accounts.

When Audit Manager removes an unlinked member account from the *accounts in scope* lists of your assessments, you aren't notified of this change. Moreover, the unlinked member account isn't notified that Audit Manager is no longer enabled on their account.

What happens if I relink a member account to my organization?

When you relink a member account to your organization, that account isn't automatically added to the scope of your existing Audit Manager assessments. However, the relinked member account now appears as an eligible AWS account when you specify the *accounts in scope* of your assessments.

- For existing assessments, you can manually edit the assessment scope to add the relinked member account. For instructions, see [Edit AWS accounts in scope](#).
- For new assessments, you can add the relinked account during assessment setup. For instructions, see [Specify AWS accounts in scope](#).

What happens if I migrate a member account from one organization to another?

If a member account has Audit Manager enabled in organization 1 and then migrates to organization 2, Audit Manager is not enabled for organization 2 as a result.

Troubleshooting evidence finder issues

Use the information on this page to resolve common evidence finder issues in Audit Manager.

General evidence finder issues

- [I can't enable evidence finder \(p. 292\)](#)
- [I enabled evidence finder, but I don't see past evidence in my search results \(p. 293\)](#)
- [I can't disable evidence finder \(p. 293\)](#)
- [My search query fails \(p. 293\)](#)

Evidence finder assessment report issues

- [I can't generate multiple assessment reports from my search results \(p. 295\)](#)
- [I can't include specific evidence from my search results \(p. 295\)](#)
- [Not all of my evidence finder results are included in the assessment report \(p. 295\)](#)
- [I want to generate an assessment report from my search results, but my query statement is failing \(p. 296\)](#)
- [More resources \(p. 298\)](#)

Evidence finder CSV export issues

- [My CSV export failed \(p. 298\)](#)
- [I can't export specific evidence from my search results \(p. 299\)](#)
- [I can't export multiple CSV files at once \(p. 299\)](#)

I can't enable evidence finder

Common reasons why you can't enable evidence finder include the following situations:

You're missing permissions

If you're trying to enable evidence finder for the first time, make sure that you have the [required permissions](#). These permissions allow you to create and manage an event data store in CloudTrail Lake, which is necessary to support evidence finder search queries. The permissions also allow you to run search queries in evidence finder.

If you need help with permissions, contact your AWS administrator. If you're an AWS administrator, you can copy the required permission statement and [attach it to an IAM policy](#).

You're using your Organizations management account

Keep in mind that you can't use your management account to enable evidence finder. Sign in as the delegated administrator account, and try again.

You previously disabled evidence finder

Re-enabling evidence finder isn't currently supported. If you previously disabled evidence finder, you can't enable it again.

I enabled evidence finder, but I don't see past evidence in my search results

When you enable evidence finder, it takes up to 7 days for all of your past evidence data to become available.

During this 7-day period, an event data store is backfilled with your past two years' worth of evidence data. This means that if you use evidence finder immediately after you enable it, not all results are available until the backfill is complete.

For instructions on how to check the status of the data backfill, see [Confirming the status of evidence finder](#).

I can't disable evidence finder

This could be caused by one of the following reasons.

You're missing permissions

If you're trying to disable evidence finder, make sure that you have the [required permissions](#). These permissions allow you to update and delete an event data store in CloudTrail Lake, which is necessary to disable evidence finder.

If you need help with permissions, contact your AWS administrator. If you're an AWS administrator, you can copy the required permission statement and [attach it to an IAM policy](#).

A request to enable evidence finder is still in progress

When you request to enable evidence finder, we create an event data store to support evidence finder queries. You can't disable evidence finder while the event data store is being created.

To proceed, wait until the event data store is created, and try again. For more information, see [Confirming the status of evidence finder](#).

You already requested to disable evidence finder

When you request to disable evidence finder, we delete the event data store that's used for evidence finder queries. If you try again to disable evidence finder while the event data store is being deleted, you get an error message.

In this case, no action is needed. Wait for the event data store to be deleted. As soon as this is complete, evidence finder is disabled. For more information, see [Confirming the status of evidence finder](#).

My search query fails

A failed search query could be caused by one of the following reasons.

You're missing permissions

Verify that the user has the [required permissions](#) to run search queries and access the search results. Specifically, you need permissions for the following CloudTrail actions:

- [StartQuery](#)
- [DescribeQuery](#)
- [CancelQuery](#)
- [GetQueryResults](#)

If you need help with permissions, contact your AWS administrator. If you're an AWS administrator, you can copy the required permission statement and [attach it to an IAM policy](#).

You're running the maximum number of queries

You can run up to 5 queries at a time. If you're running the maximum number of concurrent queries, this results in a MaxConcurrentQueriesException error. If you get this error message, wait a minute for some queries to finish, and then run the query again.

Your query statement has a validation error

If you're using the API or CLI to perform the CloudTrail Lake [StartQuery](#) operation, make sure that your queryStatement is valid. If the query statement has validation errors, incorrect syntax, or unsupported keywords, this results in an InvalidQueryStatementException.

For more information about writing a query, see [Create or edit a query](#) in the *AWS CloudTrail User Guide*.

For examples of valid syntax, review the following query statement examples that can be used to query an Audit Manager event data store.

Example 1: Investigate evidence and its compliance status

This example finds evidence with any compliance status across all assessments in account, within a specified date range.

```
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'
```

Example 2: Determine non-compliant evidence for a control

This example finds all non-compliant evidence in a specified date range for a specific assessment and control.

```
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')
```

Example 3: Count evidence by name

This example lists the total evidence for an assessment in a specified date range, grouped by name and ordered by evidence count.

```
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
```

Example 4: Explore evidence by data source and service

This example finds all evidence in a specified date range for a specific data source and service.

```
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')
```

Example 5: Explore compliant evidence by data source and control domain

This example finds compliant evidence for specific control domains, where the evidence comes from a data source that isn't 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')
```

Other API exceptions

The [StartQuery](#) API might fail for several other reasons. For a complete list of possible errors and descriptions, see [StartQuery Errors](#) in the *AWS CloudTrail API Reference*.

I can't generate multiple assessment reports from my search results

This error is caused by running too many CloudTrail Lake queries at the same time.

This error can happen if you group your search results and attempt to immediately generate assessment reports for each line item in your grouped results. When you get your search results and generate an assessment report, each action invokes a query. You can only run up to 5 queries at one time. If you're running the maximum number of concurrent queries, a `MaxConcurrentQueriesException` error is returned.

To prevent this error, make sure that you aren't generating too many assessment reports at one time. If you're running the maximum number of concurrent queries, a `MaxConcurrentQueriesException` error is returned. If you get this error message, wait a few minutes for your in-progress assessment reports to complete.

You can check the status of your assessment reports from the download center page in the Audit Manager console. After your reports are complete, return to your grouped results in evidence finder. You can then continue to get the results and generate an assessment report for each line item.

I can't include specific evidence from my search results

All of your search results are included in the assessment report. You can't selectively add individual rows from your set of search results.

If you only want to include specific search results in the assessment report, we recommend that you [edit your current search filters](#). This way, you can narrow down your results to target only the evidence that you want to include in the report.

Not all of my evidence finder results are included in the assessment report

When you generate an assessment report, there are limits for how much evidence you can add. The limit is based on the AWS Region of your assessment, the Region of the S3 bucket that's used as your assessment report destination, and whether your assessment uses a customer managed AWS KMS key.

1. The limit is 22,000 for same-Region reports (where the S3 bucket and assessment are in the same AWS Region)

2. The limit is 3,500 for cross-Region reports (where the S3 bucket and assessment are in different AWS Regions)
3. The limit is 3,500 if the assessment uses a customer managed KMS key

If you exceed this limit, the report is still created. However, Audit Manager adds only the first 3,500 or 22,000 evidence items to the report.

To prevent this issue, we recommend that you [edit your current search filters](#). This way, you can reduce your search results by targeting a smaller amount of evidence. If needed, you can repeat this method and generate multiple assessment reports instead of one larger report.

I want to generate an assessment report from my search results, but my query statement is failing

If you're using the [CreateAssessmentReport](#) API and your query statement returns a validation exception, check the table below for guidance on how to fix it.

Note

Even if a query statement works in CloudTrail, the same query might not be valid for assessment report generation in Audit Manager. This is because of some differences in query validation between the two services.

Clause	Issue	Solution	Notes
SELECT	The SELECT clause contains a column name	Remove the SELECT clause and replace with SELECT eventJson.	Only SELECT eventJson is supported. This validation is handled by Audit Manager.
FROM	The FROM clause contains an invalid event data store ID or The provided event data store ID doesn't match the event data store ID in your Audit Manager settings	Remove the FROM clause and replace with FROM <i>edsID</i> , where the value of edsID matches the event data store ID that's specified in your Audit Manager settings. You can retrieve the ARN of the event data store from your Audit Manager settings. For more information, see GetSettings in the <i>AWS Audit Manager API Reference</i> .	This validation is handled by Audit Manager.
GROUP BY	A GROUP BY clause is present in the query	Remove the GROUP BY clause.	This validation is handled by Audit Manager.
HAVING	A HAVING clause is present in the query	Remove the HAVING clause.	This validation is handled by Audit Manager.
LIMIT	The LIMIT clause contains a value that exceeds the maximum allowed limit	If the LIMIT clause exists, ensure that its value is equal to or less than the maximum supported limit: <ul style="list-style-type: none">• For same-Region reports, the limit is 22,000	In the console, there's no limit to the number of evidence results that can be returned. However, when generating an assessment report, a limit applies to the amount of evidence that you can include.

Clause	Issue	Solution	Notes
		<ul style="list-style-type: none"> For cross-Region reports, the limit is 3,500 For reports where the related assessment uses a customer managed AWS KMS key, the limit is 3,500 	If no LIMIT value is provided in your query statement, the default maximum limits are applied. This validation is handled by Audit Manager.
ORDER BY	The ORDER BY clause contains Aggregate functions or Aliases that aren't present in the SELECT clause	Ensure that the ORDER BY clause doesn't contain any conditions using Aggregate functions or Aliases .	This validation is handled by the CloudTrail StartQuery API .
WHERE	The WHERE clause contains more than one assessmentId or The WHERE clause contains an assessmentId that doesn't match the assessmentId in your <code>createAssessmentReport</code> request or The WHERE clause contains an unsupported column name	Ensure that only one assessmentID is specified, and that it matches the assessmentId parameter that you specified in the <code>createAssessmentReport</code> API request. Remove any unsupported column names.	This validation is handled by the CloudTrail StartQuery API .

Examples

The following examples show how you can use the `queryStatement` parameter when calling the [CreateAssessmentReport](#) operation. Before you use these queries, replace the `placeholder text` with your own `edsId` and `assessmentId` values.

Example 1: Create a report (same-Region limit applies)

This example creates a report that includes results for S3 buckets created between January 22-23rd, 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
```

Example 2: Create a report (cross-Region limit applies)

This example creates a report that includes all results for the specified event data store and assessment, with no date range specified.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId =  
'11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 7000
```

Example 3: Create a report (under the default limit)

This example creates a report that includes all results for the specified event data store and assessment, with a limit that's under the default maximum.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId =  
'11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 2000
```

More resources

The following page contains general troubleshooting guidance about assessment reports:

- [Troubleshooting assessment report issues](#)

My CSV export failed

Your CSV export might fail for a number of reasons. You can troubleshoot this issue by checking the most frequent causes.

First, make sure that you meet the prerequisites for using the CSV export feature:

You successfully enabled evidence finder

If you haven't [enabled evidence finder](#), you can't run a search query and export your search results.

The backfill of your event data store is complete

If you use evidence finder immediately after you enable it, and the [evidence backfill](#) is still in progress, there may be some results that aren't available. To check the backfill status, see [Confirm the status of evidence finder](#).

Your search query succeeded

Audit Manager can't export the results of a failed query. To troubleshoot a failed query, see [My search query fails \(p. 293\)](#).

After you've confirmed that you meet the prerequisites, use the following checklist to check for potential issues:

1. Check the status of your search query:
 - a. **Was the query cancelled?** Evidence finder displays partial results that were processed before the query was cancelled. However, Audit Manager doesn't export partial results to your S3 bucket or the download center.
 - b. **Has the query been running for over one hour?** Queries that run for longer than one hour might time out. Evidence finder displays partial results that were processed before the query timed out. However, Audit Manager doesn't export partial results. To avoid a timeout, you can reduce the amount of evidence that's scanned by [editing your search query](#) to specify a narrower time range.
2. Check the name and the URI of your export destination S3 bucket:
 - a. **Does the bucket that you specified exist?** If you manually entered a bucket URI, make sure that you didn't mistype anything. A typo or an incorrect URI can result in a RESOURCE_NOT_FOUND error when Audit Manager attempts to export the CSV file to Amazon S3.
3. Check the permissions of your export destination S3 bucket:

- a. **Do you have write permissions for the S3 bucket?** You must have write access for the S3 bucket that you're using as the export destination. More specifically, the IAM permissions policy must include an s3:PutObject action and the bucket ARN, and list CloudTrail as the service principal. We provide an [example policy](#) that you can use. For instructions on how to use a different S3 bucket, see [Export destination settings](#).
4. Check if any of your AWS Region information doesn't match up:
 - a. **Does the AWS Region of your customer managed key match the AWS Region of your assessment?** If you provided a customer managed key for data encryption, it must be in the same AWS Region as your assessment. For instructions on how to change the KMS key, see [Data encryption settings](#).
5. Check the permissions of your delegated administrator account:
 - a. **Does the customer managed key in your Audit Manager settings grant permissions to your delegated administrator?** If you're using a delegated administrator account and you specified a customer managed key for data encryption, make sure the delegated administrator has access on that KMS key. For instructions, see [Allowing users in other accounts to use a KMS key](#) in the *AWS Key Management Service Developer Guide*. To review and change your encryption settings in Audit Manager, see [Data encryption settings](#).

Note

If you change your Audit Manager data encryption settings, these changes apply to new assessments that you create moving forward. This includes any CSV files that you export from your new assessments.

The changes don't apply to existing assessments that you created before you changed your encryption settings. This includes new CSV exports from existing assessments, in addition to existing CSV exports. Existing assessments—and all their CSV exports—continue to use the old KMS key. If the IAM identity that's exporting the CSV file doesn't have permissions to use the old KMS key, you can grant permissions at the key policy level.

I can't export specific evidence from my search results

All of your search results are included in the results.

If you want to include only specific evidence in the CSV file, we recommend that you [edit your current search filters](#). This way, you can narrow your results to target only the evidence that you want to export.

I can't export multiple CSV files at once

This error is caused by running too many CloudTrail Lake queries at the same time.

This can happen if you group your search results and attempt to immediately export a CSV file for each line item in your grouped results. When you get your search results and export a CSV file, each of these actions invokes a query. You can run only up to five queries at one time. If you're running the maximum number of concurrent queries, a `MaxConcurrentQueriesException` error is returned.

To prevent this error, make sure that you aren't exporting too many CSV files at one time.

To resolve this error, wait for your in-progress CSV exports to complete. Most exports take a few minutes. However, if you're exporting a very large amount of data, it might take up to an hour to complete the export. Feel free to navigate away from evidence finder while the export is in progress.

You can check the export status from the download center in the Audit Manager console. After your exported files are ready, return to your grouped results in evidence finder. You can then continue to get the results and export a CSV file for each line item.

Troubleshooting framework sharing issues

You can use the information on this page to resolve common framework sharing issues in Audit Manager.

Topics

- [My sent share request status displays as Failed \(p. 300\)](#)
- [My share request has a blue dot next to it. What does this mean? \(p. 300\)](#)
- [My shared framework has controls that use custom AWS Config rules as a data source. Can the recipient collect evidence for these controls? \(p. 302\)](#)
- [I updated a custom rule that's used in a shared framework. Do I need to take any action? \(p. 303\)](#)

My sent share request status displays as *Failed*

If you try to share a custom framework and the operation fails, we recommend that you check the following:

1. Make sure that Audit Manager is enabled in the recipient's AWS account and in the specified Region. For a list of supported AWS Audit Manager Regions, see [AWS Audit Manager endpoints and quotas](#) in the *Amazon Web Services General Reference*.
2. Make sure that you entered the correct AWS account ID when you specified the recipient account.
3. Make sure that you didn't specify an AWS Organizations management account as the recipient. You can share a custom framework with a delegated administrator, but if you try to share a custom framework with a management account, the operation fails.
4. If you use a customer managed key to encrypt your Audit Manager data, make sure that your KMS key is enabled. If your KMS key is disabled and you try to share a custom framework, the operation fails. For instructions on how to enable a disabled KMS key, see [Enabling and disabling keys](#) in the *AWS Key Management Service Developer Guide*.

My share request has a blue dot next to it. What does this mean?

A blue dot notification indicates that a share request needs your attention.

Blue dot notifications for senders

A blue notification dot appears next to sent share requests with a status of *Expiring*. Audit Manager displays the blue dot notification so that you can remind the recipient to take action on the share request before it expires.

For the blue notification dot to disappear, the recipient must accept or decline the request. The blue dot also disappears if you revoke the share request.

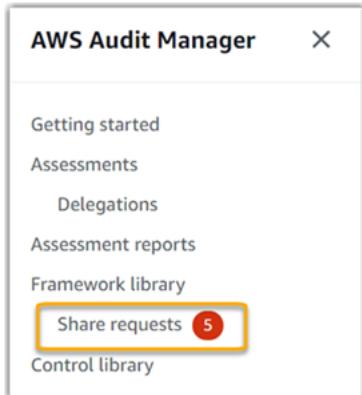
You can use the following procedure to check for any expiring share requests, and send an optional reminder to the recipient to take action.

To view notifications for sent requests

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. If you have a share request notification, Audit Manager displays a red dot next to the navigation menu icon.



3. Expand the navigation pane and look next to **Share requests**. A notification badge indicates the number of share requests that need attention.



4. Choose **Share requests**, and then choose the **Sent requests** tab.
5. Look for the blue dot to identify share requests that expire within the next 30 days. Alternatively, you can also view expiring share requests by selecting **Expiring** from the **All statuses** filter dropdown.

Sent requests (19) Info			
<input type="text"/> Search			
Framework name	Request status	Expiration date	
<input type="radio"/> FrameworkShare-CustomStandardMix	<input checked="" type="radio"/> Expiring	January 11, 2022, 5:13 PM UTC	

6. (Optional) Remind the recipient that they need to take action on the share request before it expires. This step is optional, as Audit Manager sends a notification in the console to inform the recipient when a share request is active or expiring. However, you can also send your own reminder to the recipient using your preferred communication channel.

Blue dot notifications for recipients

A blue notification dot appears next to received share requests with a status of *Active* or *Expiring*. Audit Manager displays the blue dot notification to remind you to take action on the share request before it expires. For the blue notification dot to disappear, you must [accept or decline](#) the request. The blue dot also disappears if the sender revokes the share request.

You can use the following procedure to check for active and expiring share requests.

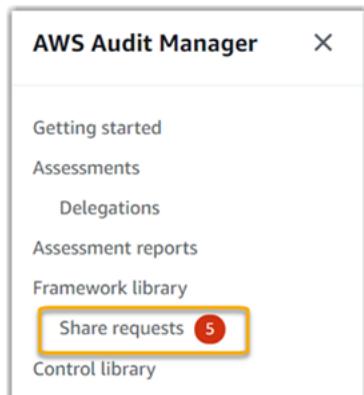
To view notifications for received requests

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. If you have a share request notification, Audit Manager displays a red dot next to the navigation menu icon.



My shared framework has controls that use custom AWS Config rules as a data source. Can the recipient collect evidence for these controls?

3. Expand the navigation pane and look next to **Share requests**. A notification badge indicates the number of share requests that need your attention.



4. Choose **Share requests**. By default, this page opens on the **Received requests** tab.
5. Identify the share requests that need your action by looking for items with a blue dot.

Received requests (21) Info			
<input type="text"/> Search	All statuses	Framework name	Request status
<input type="radio"/>	<input checked="" type="radio"/>	FrameworkShare-CustomStandardMix	<input checked="" type="radio"/> Active January 11, 2022, 8:37 AM UTC
<input type="radio"/>	<input checked="" type="radio"/>	FrameworkShare-CustomStandardMix	<input checked="" type="radio"/> Active January 11, 2022, 8:35 AM UTC

6. (Optional) To view only requests that expire in the next 30 days, find the **All statuses** dropdown list and select **Expiring**.

My shared framework has controls that use custom AWS Config rules as a data source. Can the recipient collect evidence for these controls?

Yes, your recipient can collect evidence for these controls, but a few steps are needed to achieve this.

For Audit Manager to collect evidence using an AWS Config rule as a data source mapping, the following must be true. These criteria apply to both managed rules and custom rules.

- The rule must exist in the recipient's AWS environment.
- The rule must be enabled in the recipient's AWS environment.

Remember that the AWS Config rules in your account likely don't exist already in the recipient's AWS environment. Moreover, when the recipient accepts the share request, Audit Manager doesn't recreate any of your custom rules in their account. For the recipient to collect evidence using your custom rules as a data source mapping, they must create the same custom rules in their instance of AWS Config. After the recipient creates and then enables the rules in AWS Config, Audit Manager can collect evidence from that data source.

We recommend that you communicate with the recipient to let them know if any custom AWS Config rules should be created in their instance of AWS Config.

I updated a custom rule that's used in a shared framework. Do I need to take any action?

For rule updates within your AWS environment

When you update a custom rule within your AWS environment, no action is needed in Audit Manager. Audit Manager detects and handles rule updates in the way that's described in the following table. Audit Manager doesn't notify you when a rule update is detected.

Scenario	What Audit Manager does	What you need to do
A custom rule is updated in your instance of AWS Config.	Audit Manager continues to report findings for that rule using the updated rule definition.	No action is needed.
A custom rule is deleted in your instance of AWS Config.	Audit Manager stops reporting findings for the deleted rule.	No action is needed. If you want to, you can edit the custom controls that used the deleted rule as a data source mapping. You can then remove the deleted rule to clean up your control's data source settings. Otherwise, the deleted rule name remains as an unused data source mapping.

For rule updates outside your AWS environment

In the recipient's AWS environment, Audit Manager doesn't detect the rule update. This is because senders and recipients each work in separate AWS environments. The following table provides recommended actions for this scenario.

Your role	Scenario	Recommended action
Sender	<ul style="list-style-type: none">You shared a framework that uses custom rules as a data source mapping.After you shared the framework, you updated or deleted one of those rules in AWS Config.	Contact the recipient to let them know about the update. That way, they can make the same update and stay in sync with the latest rule definition.
Recipient	<ul style="list-style-type: none">You accepted a shared framework that uses custom rules as a data source mapping.After you recreated the custom rules in your instance of AWS Config, the sender updated or deleted one of those rules.	Make the corresponding rule update in your own instance of AWS Config.

Troubleshooting notification issues

You can use the information on this page to resolve common notification issues in Audit Manager.

Topics

- [I specified an Amazon SNS topic in Audit Manager, but I'm not receiving any notifications \(p. 304\)](#)
- [I specified a FIFO topic, but I'm not receiving notifications in the expected order \(p. 304\)](#)

I specified an Amazon SNS topic in Audit Manager, but I'm not receiving any notifications

If your Amazon SNS topic uses AWS KMS for server-side encryption (SSE), you might be missing the required permissions for your AWS KMS key policy. You might also fail to receive notifications if you didn't subscribe an endpoint to your topic.

If you aren't receiving notifications, make sure that you did the following:

- You attached the required permissions policy to your KMS key. An example policy is available on the [Notifications](#) page of this guide.
- You subscribed an endpoint to the topic that the notifications are sent through. When you subscribe an email endpoint to a topic, you receive an email asking you to confirm your subscription. You must confirm your subscription to start receiving email notifications. For more information, see [Getting Started](#) in the Amazon SNS Developer Guide.

I specified a FIFO topic, but I'm not receiving notifications in the expected order

Audit Manager supports sending notifications to FIFO SNS topics. However, the order in which Audit Manager sends notifications to your FIFO topics isn't guaranteed.

Troubleshooting permission and access issues

You can use the information on this page to resolve common permission issues in Audit Manager.

Topics

- [I followed the Audit Manager setup procedure, but I don't have enough IAM privileges \(p. 304\)](#)
- [I specified someone as an audit owner, but they still don't have full access to the assessment. Why is this? \(p. 305\)](#)
- [I can't perform an action in Audit Manager \(p. 305\)](#)
- [I want to allow people outside of my AWS account to access my Audit Manager resources \(p. 305\)](#)
- [See also \(p. 282\)](#)

I followed the Audit Manager setup procedure, but I don't have enough IAM privileges

The user, role, or group that you use to access Audit Manager must have the required permissions. Moreover, your identity-based policy shouldn't be too restrictive. Otherwise, the console won't function as intended. The [Setting up](#) procedure in this guide provides a policy that grants the minimum permissions needed to set up Audit Manager. Depending on your use case, you might need broader, less restrictive permissions. For example, we recommend that audit owners have [administrator access](#). This is

I specified someone as an audit owner, but they still don't have full access to the assessment. Why is this?

so that they can modify Audit Manager settings and manage resources such as assessments, frameworks, controls, and assessment reports. Other users, such as delegates, might only need [management access or read-only](#) access.

Make sure that you add the appropriate permissions for your user, role, or group. For audit owners, the recommended policy is [AWSAuditManagerAdministratorAccess](#). For delegates, you can use [this example](#) that's provided on the [IAM policy examples](#) page. You can use these example policies as a starting point, and make changes as necessary to fit your requirements.

We recommend that you take time to customize your permissions to meet your specific requirements. If you need help with IAM permissions, contact your administrator or [AWS Support](#).

I specified someone as an audit owner, but they still don't have full access to the assessment. Why is this?

Specifying someone as an audit owner alone doesn't provide them with full access to an assessment. Audit owners must also have the necessary IAM permissions to access and manage Audit Manager resources. In other words, in addition to [specifying a user as an audit owner](#), you must also attach the necessary [IAM policies](#) to that user. The idea behind this is that, by requiring both, Audit Manager ensures that you have full control over all of the specifics of each assessment.

Note

For audit owners, we recommend that you use the [AWSAuditManagerAdministratorAccess](#) policy. For more information, see [Recommended policies for user personas in Audit Manager](#).

I can't perform an action in Audit Manager

If you don't have the necessary permissions to use the AWS Audit Manager console or Audit Manager API operations, you will likely encounter an `AccessDeniedException` error.

To resolve this issue, you must contact your administrator for assistance. Your administrator is the person that provided you with your sign-in credentials.

I want to allow people outside of my AWS account to access my Audit Manager resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Audit Manager supports these features, see [How AWS Audit Manager works with IAM \(p. 316\)](#).
- To learn how to provide access to your resources across AWS accounts that you own, see [Providing access to an IAM user in another AWS account that you own](#) in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see [Providing access to AWS accounts owned by third parties](#) in the *IAM User Guide*.
- To learn how to provide access through identity federation, see [Providing access to externally authenticated users \(identity federation\)](#) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see [How IAM roles differ from resource-based policies](#) in the *IAM User Guide*.

See also

The following pages contain troubleshooting guidance for other issues that can be caused by missing permissions:

- [I can't see any controls or control sets in my assessment](#)
- [The custom rule option is unavailable when I'm configuring a control data source](#)
- [I get an *access denied* error when I try to generate an assessment report](#)
- [I get an *access denied* error when I try to generate an assessment report using my delegated administrator account](#)
- [I can't enable evidence finder](#)
- [I can't disable evidence finder](#)
- [My search query fails in evidence finder](#)
- [I specified an Amazon SNS topic in Audit Manager, but I'm not receiving any notifications](#)

Quotas and restrictions for AWS Audit Manager

Your AWS account has default quotas, formerly referred to as *limits*, for each AWS service. Unless otherwise noted, each quota is Region-specific. You can request increases for some quotas, and other quotas can't be increased.

Most Audit Manager quotas, but not all, are listed under the AWS Audit Manager namespace in the Service Quotas console. To learn how to request a quota increase, see [Managing your Audit Manager quotas \(p. 308\)](#).

Default Audit Manager quotas

The following AWS Audit Manager quotas are per AWS account per Region.

Assessments

- Number of active assessments per account: 100

Assessment reports

- Number of evidence items that you can add to an assessment report:
 - For same-Region reports (where the assessment and the assessment report destination S3 bucket are in the same AWS Region): 22,000
 - For cross-Region reports (where the assessment and the assessment report destination S3 bucket are in different AWS Regions): 3,500
 - For reports where the related assessment uses a customer managed AWS KMS key: 3,500

Controls

- Number of custom controls per account: 500

Evidence

- Maximum size of a single manual evidence file: 100 MB
- Number of daily manual evidence uploads per control: 100

Tip

If you need to upload a large amount of manual evidence to a single control, we recommend that you upload your evidence in batches across several days.

Frameworks

- Number of custom frameworks per account: 100

Note

Framework quotas apply to all shared custom frameworks in your framework library, regardless of who created the framework.

Shared custom framework recipients

- Number of active recipient accounts: 100

API access

- Number of transactions per second (TPS) across all APIs: 20 TPS

Managing your Audit Manager quotas

AWS Audit Manager is integrated with Service Quotas, an AWS service that enables you to view and manage your quotas from a central location. For more information, see [What Is Service Quotas?](#) in the *Service Quotas User Guide*. Service Quotas makes it easy to look up the value of your Audit Manager quotas.

To view Audit Manager service quotas using the console

1. Open the Service Quotas console at <https://console.aws.amazon.com/servicequotas/>.
2. In the navigation pane, choose **AWS services**.
3. From the **AWS services** list, search for and select **AWS Audit Manager**.
4. In the **Service quotas** list, you can see the service quota name, applied quota value (if it's available), AWS default quota value, and whether the quota is adjustable.
5. To view additional information about a service quota, such as the description, choose the quota name.
6. (Optional) To request a quota increase, select the quota that you want to increase, select **Request quota increase**, enter or select the required information, and select **Request**.

For more information, see [Requesting a quota increase](#) in the *Service Quotas User Guide*.

Security in AWS Audit Manager

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from data centers and network architectures that are built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The [shared responsibility model](#) describes this as security of the cloud and security *in the cloud*:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the [AWS Compliance Programs](#). To learn about the compliance programs that apply to AWS Audit Manager, see [AWS Services in Scope by Compliance Program](#).
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using AWS Audit Manager. The following topics show you how to configure Audit Manager to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Audit Manager resources.

Topics

- [Data protection in AWS Audit Manager \(p. 309\)](#)
- [Identity and access management for AWS Audit Manager \(p. 312\)](#)
- [Compliance validation for AWS Audit Manager \(p. 358\)](#)
- [Resilience in AWS Audit Manager \(p. 359\)](#)
- [Infrastructure security in AWS Audit Manager \(p. 359\)](#)
- [AWS Audit Manager and interface VPC endpoints \(AWS PrivateLink\) \(p. 359\)](#)
- [Logging and monitoring in AWS Audit Manager \(p. 361\)](#)
- [Configuration and vulnerability analysis in AWS Audit Manager \(p. 366\)](#)

Data protection in AWS Audit Manager

The AWS [shared responsibility model](#) applies to data protection in AWS Audit Manager. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. This content includes the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the [Data Privacy FAQ](#). For information about data protection in Europe, see the [AWS Shared Responsibility Model and GDPR](#) blog post on the [AWS Security Blog](#).

For data protection purposes, we recommend that you protect AWS account credentials and set up individual users with AWS IAM Identity Center or AWS Identity and Access Management (IAM). That way, each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We require TLS 1.2 and recommend TLS 1.3.
- Set up API and user activity logging with AWS CloudTrail.

- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon S3.
- If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see [Federal Information Processing Standard \(FIPS\) 140-2](#).

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text fields such as a **Name** field. This includes when you work with Audit Manager or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

In addition to the recommendation above, we recommend specifically that Audit Manager customers don't include sensitive identifying information in free-form fields when creating assessments, custom controls, custom frameworks, and delegation comments.

Deletion of Audit Manager data

There are several ways that Audit Manager data can be deleted.

Data deletion when disabling Audit Manager

When you [disable Audit Manager](#), you can decide if you want to delete all of your Audit Manager data. If you choose to delete your data, it's deleted within 7 days of disabling Audit Manager. After your data is deleted, you can't recover it.

Automatic data deletion

Some Audit Manager data is deleted automatically after a specific period of time. Audit Manager retains customer data as follows.

Data type	Data retention period	Notes
Evidence	Data is retained for 2 years from the time of creation	Includes automated evidence and manual evidence
Customer-created resources	Data is retained indefinitely	Includes assessments, assessment reports, custom controls, and custom frameworks

Manual data deletion

You can delete individual Audit Manager resources at any time. For instructions, see the following:

- [Deleting an assessment](#)
 - See also: [DeleteAssessment](#) in the *AWS Audit Manager API Reference*
- [Deleting a custom framework](#)
 - See also: [DeleteAssessmentFramework](#) in the *AWS Audit Manager API Reference*
- [Deleting a share request](#)
 - See also: [DeleteAssessmentFrameworkShare](#) in the *AWS Audit Manager API Reference*

- [Deleting an assessment report](#)
 - See also: [DeleteAssessmentReport](#) in the *AWS Audit Manager API Reference*
- [Deleting a custom control](#)
 - See also: [DeleteControl](#) in the *AWS Audit Manager API Reference*

To delete other resource data that you might have created when using Audit Manager, see the following:

- [Delete an event data store](#) in the *AWS CloudTrail User Guide*
- [Deleting a bucket](#) in the *Amazon Simple Storage Service (Amazon S3) User Guide*

Encryption at rest

To encrypt data at rest, Audit Manager uses server-side encryption with AWS managed keys for all its data stores and logs.

Your data is encrypted under a customer managed key or an AWS owned key, depending on your selected settings. If you don't provide a customer managed key, Audit Manager uses an AWS owned key to encrypt your content. All service metadata in DynamoDB and Amazon S3 in Audit Manager is encrypted using an AWS owned key.

Audit Manager encrypts data as follows:

- Service metadata stored in Amazon S3 is encrypted under an AWS owned key using SSE-KMS.
- Service metadata stored in DynamoDB is server side encrypted using KMS and an AWS owned key.
- Your content stored in DynamoDB is client-side encrypted using either a customer managed key or an AWS owned key. The KMS key is based on your chosen settings.
- Your content stored in Amazon S3 in Audit Manager is encrypted using SSE-KMS. The KMS key is based on your selection, and could be either a customer managed key or an AWS owned key.
- The assessment reports published to your S3 bucket are encrypted as follows:
 - If you provided a customer managed key, your data is encrypted using SSE-KMS.
 - If you used the AWS owned key, your data is encrypted using SSE-S3.

Encryption in transit

Audit Manager provides secure and private endpoints for encrypting data in transit. The secure and private endpoints allow AWS to protect the integrity of API requests to Audit Manager.

Inter-service transit

By default, all inter-service communications are protected by using Transport Layer Security (TLS) encryption.

Key management

Audit Manager supports both AWS owned keys and customer managed keys for encrypting all Audit Manager resources (assessments, controls, frameworks, evidence, and assessment reports saved to S3 buckets in your accounts).

We recommend that you use a customer managed key. By doing so, you can view and manage the encryption keys that protect your data, including viewing logs of their use in AWS CloudTrail. When you choose a customer managed key, Audit Manager creates a grant on the KMS key so that it can be used to encrypt your content.

Warning

After you delete or disable a KMS key that is used to encrypt Audit Manager resources, you can no longer decrypt the resource that was encrypted under that KMS key, which means that data becomes unrecoverable.

Deleting a KMS key in AWS Key Management Service (AWS KMS) is destructive and potentially dangerous. For more information about deleting KMS keys, see [Deleting AWS KMS keys](#) in the [AWS Key Management Service User Guide](#).

You can specify your encryption settings when you enable Audit Manager using the AWS Management Console, the Audit Manager API, or the AWS Command Line Interface (AWS CLI). For instructions, see [Enable AWS Audit Manager \(p. 28\)](#).

You can review and change your encryption settings at any time. For instructions, see [Data encryption \(p. 252\)](#).

For more information about how to set up customer managed keys, see [Creating keys](#) in the [AWS Key Management Service User Guide](#).

Identity and access management for AWS Audit Manager

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use Audit Manager resources. IAM is an AWS service that you can use with no additional charge.

Topics

- [Audience \(p. 312\)](#)
- [Authenticating with identities \(p. 313\)](#)
- [Managing access using policies \(p. 315\)](#)
- [How AWS Audit Manager works with IAM \(p. 316\)](#)
- [Identity-based policy examples for AWS Audit Manager \(p. 323\)](#)
- [Cross-service confused deputy prevention \(p. 336\)](#)
- [AWS managed policies for AWS Audit Manager \(p. 337\)](#)
- [Troubleshooting AWS Audit Manager identity and access \(p. 350\)](#)
- [Using service-linked roles for AWS Audit Manager \(p. 351\)](#)

Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work that you do in Audit Manager.

Service user – If you use the Audit Manager service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Audit Manager features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator. If you cannot access a feature in Audit Manager, see [Troubleshooting AWS Audit Manager identity and access \(p. 350\)](#).

Service administrator – If you're in charge of Audit Manager resources at your company, you probably have full access to Audit Manager. It's your job to determine which Audit Manager features and resources your service users should access. You must then submit requests to your IAM administrator to change the

permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with Audit Manager, see [How AWS Audit Manager works with IAM \(p. 316\)](#).

IAM administrator – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to Audit Manager. To view example Audit Manager identity-based policies that you can use in IAM, see [Identity-based policy examples for AWS Audit Manager \(p. 323\)](#).

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. You must be *authenticated* (signed in to AWS) as the AWS account root user, as an IAM user, or by assuming an IAM role.

You can sign in to AWS as a federated identity by using credentials provided through an identity source. AWS IAM Identity Center (IAM Identity Center) users, your company's single sign-on authentication, and your Google or Facebook credentials are examples of federated identities. When you sign in as a federated identity, your administrator previously set up identity federation using IAM roles. When you access AWS by using federation, you are indirectly assuming a role.

Depending on the type of user you are, you can sign in to the AWS Management Console or the AWS access portal. For more information about signing in to AWS, see [How to sign in to your AWS account](#) in the *AWS Sign-In User Guide*.

If you access AWS programmatically, AWS provides a software development kit (SDK) and a command line interface (CLI) to cryptographically sign your requests by using your credentials. If you don't use AWS tools, you must sign requests yourself. For more information about using the recommended method to sign requests yourself, see [Signing AWS API requests](#) in the *IAM User Guide*.

Regardless of the authentication method that you use, you might be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see [Multi-factor authentication](#) in the *AWS IAM Identity Center User Guide* and [Using multi-factor authentication \(MFA\) in AWS](#) in the *IAM User Guide*.

AWS account root user

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see [Tasks that require root user credentials](#) in the *IAM User Guide*.

Federated identity

As a best practice, require human users, including users that require administrator access, to use federation with an identity provider to access AWS services by using temporary credentials.

A *federated identity* is a user from your enterprise user directory, a web identity provider, the AWS Directory Service, the Identity Center directory, or any user that accesses AWS services by using credentials provided through an identity source. When federated identities access AWS accounts, they assume roles, and the roles provide temporary credentials.

For centralized access management, we recommend that you use AWS IAM Identity Center. You can create users and groups in IAM Identity Center, or you can connect and synchronize to a set of users and groups in your own identity source for use across all your AWS accounts and applications. For information about IAM Identity Center, see [What is IAM Identity Center?](#) in the *AWS IAM Identity Center User Guide*.

IAM users and groups

An [IAM user](#) is an identity within your AWS account that has specific permissions for a single person or application. Where possible, we recommend relying on temporary credentials instead of creating IAM users who have long-term credentials such as passwords and access keys. However, if you have specific use cases that require long-term credentials with IAM users, we recommend that you rotate access keys. For more information, see [Rotate access keys regularly for use cases that require long-term credentials](#) in the *IAM User Guide*.

An [IAM group](#) is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named *IAMAdmins* and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see [When to create an IAM user \(instead of a role\)](#) in the *IAM User Guide*.

IAM roles

An [IAM role](#) is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by [switching roles](#). You can assume a role by calling an AWS CLI or AWS API operation or by using a custom URL. For more information about methods for using roles, see [Using IAM roles](#) in the *IAM User Guide*.

IAM roles with temporary credentials are useful in the following situations:

- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see [Creating a role for a third-party Identity Provider](#) in the *IAM User Guide*. If you use IAM Identity Center, you configure a permission set. To control what your identities can access after they authenticate, IAM Identity Center correlates the permission set to a role in IAM. For information about permissions sets, see [Permission sets](#) in the *AWS IAM Identity Center User Guide*.
- **Temporary IAM user permissions** – An IAM user or role can assume an IAM role to temporarily take on different permissions for a specific task.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see [How IAM roles differ from resource-based policies](#) in the *IAM User Guide*.
- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
 - **Principal permissions** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. Policies grant permissions to a principal. When you use some services, you might perform an action that then triggers another action in a different service. In this case, you must have permissions to perform both actions. To see whether an action requires additional dependent actions in a policy, see [Actions, Resources, and Condition Keys for AWS Audit Manager](#) in the *Service Authorization Reference*.
 - **Service role** – A service role is an [IAM role](#) that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see [Creating a role to delegate permissions to an AWS service](#) in the *IAM User Guide*.

- **Service-linked role** – A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.
- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see [Using an IAM role to grant permissions to applications running on Amazon EC2 instances](#) in the *IAM User Guide*.

To learn whether to use IAM roles or IAM users, see [When to create an IAM role \(instead of a user\)](#) in the *IAM User Guide*.

Managing access using policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when a principal (user, root user, or role session) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see [Overview of JSON policies](#) in the *IAM User Guide*.

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

By default, users and roles have no permissions. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see [Creating IAM policies](#) in the *IAM User Guide*.

Identity-based policies can be further categorized as *inline policies* or *managed policies*. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see [Choosing between managed policies and inline policies](#) in the *IAM User Guide*.

Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must [specify a principal](#) in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

Access control lists (ACLs)

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs. To learn more about ACLs, see [Access control list \(ACL\) overview](#) in the *Amazon Simple Storage Service Developer Guide*.

Other policy types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of an entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the Principal field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see [Permissions boundaries for IAM entities](#) in the *IAM User Guide*.
- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see [How SCPs work](#) in the *AWS Organizations User Guide*.
- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see [Session policies](#) in the *IAM User Guide*.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see [Policy evaluation logic](#) in the *IAM User Guide*.

How AWS Audit Manager works with IAM

Before you use IAM to manage access to Audit Manager, learn what IAM features are available to use with Audit Manager.

IAM features you can use with AWS Audit Manager

IAM feature	Audit Manager support
Identity-based policies (p. 317)	Yes

IAM feature	Audit Manager support
Resource-based policies (p. 318)	No
Policy actions (p. 318)	Yes
Policy resources (p. 319)	Yes
Policy condition keys (p. 320)	Partial
ACLs (p. 321)	No
ABAC (tags in policies) (p. 321)	Yes
Temporary credentials (p. 322)	Yes
Principal permissions (p. 322)	Yes
Service roles (p. 322)	No
Service-linked roles (p. 322)	Yes

To get a high-level view of how AWS Audit Manager and other AWS services work with most IAM features, see [AWS services that work with IAM](#) in the *IAM User Guide*.

Identity-based policies for AWS Audit Manager

Supports identity-based policies	Yes
----------------------------------	-----

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see [Creating IAM policies](#) in the *IAM User Guide*.

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. You can't specify the principal in an identity-based policy because it applies to the user or role to which it is attached. To learn about all of the elements that you can use in a JSON policy, see [IAM JSON policy elements reference](#) in the *IAM User Guide*.

AWS Audit Manager creates a managed policy named `AWSAuditManagerAdministratorAccess` for Audit Manager administrators. This policy grants full administration access in Audit Manager. Administrators can attach this policy to any existing role or user, or create a new role with this policy.

Recommended policies for user personas in AWS Audit Manager

AWS Audit Manager enables you to maintain the segregation of duties among different users and for different audits by using different IAM policies. The two personas in Audit Manager and their recommended policies are defined as follows.

Persona	Description and recommended policy
Audit owner	<ul style="list-style-type: none"> This persona must have the necessary permissions to manage assessments in AWS Audit Manager. The recommended policy to use for this persona is the managed policy named AWSAuditManagerAdministratorAccess. You can use this policy as a starting point, and scope down these permissions as needed to fit your requirements.

Persona	Description and recommended policy
Delegate	<ul style="list-style-type: none">This persona can access the delegated control sets in an assessment. They can update the control status, add comments, submit a control set for review, and add evidence to the assessment report.The recommended policy to use for this persona is the following example policy: Allow users full administrator access to AWS Audit Manager (p. 325). You can use this policy as a starting point, and make changes as necessary to fit your requirements.

Identity-based policy examples for AWS Audit Manager

To view examples of Audit Manager identity-based policies, see [Identity-based policy examples for AWS Audit Manager \(p. 323\)](#).

Resource-based policies within AWS Audit Manager

Supports resource-based policies	No
----------------------------------	----

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must [specify a principal](#) in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

To enable cross-account access, you can specify an entire account or IAM entities in another account as the principal in a resource-based policy. Adding a cross-account principal to a resource-based policy is only half of establishing the trust relationship. When the principal and the resource are in different AWS accounts, an IAM administrator in the trusted account must also grant the principal entity (user or role) permission to access the resource. They grant permission by attaching an identity-based policy to the entity. However, if a resource-based policy grants access to a principal in the same account, no additional identity-based policy is required. For more information, see [How IAM roles differ from resource-based policies](#) in the *IAM User Guide*.

Policy actions for AWS Audit Manager

Supports policy actions	Yes
-------------------------	-----

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The Action element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Policy actions usually have the same name as the associated AWS API operation. There are some exceptions, such as *permission-only actions* that don't have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called *dependent actions*.

Include actions in a policy to grant permissions to perform the associated operation.

To see a list of AWS Audit Manager actions, see [Actions defined by AWS Audit Manager](#) in the *Service Authorization Reference*.

Policy actions in AWS Audit Manager use the following prefix before the action.

```
auditmanager
```

To specify multiple actions in a single statement, separate them with commas.

```
"Action": [  
    "auditmanager:GetEvidenceDetails",  
    "auditmanager:GetEvidenceEventDetails"  
]
```

You can specify multiple actions using wildcards (*). For example, to specify all actions that begin with the word Get, include the following action.

```
"Action": "auditmanager:Get*"
```

To view examples of Audit Manager identity-based policies, see [Identity-based policy examples for AWS Audit Manager \(p. 323\)](#).

Policy resources for AWS Audit Manager

Supports policy resources	Yes
---------------------------	-----

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The Resource JSON policy element specifies the object or objects to which the action applies. Statements must include either a Resource or a NotResource element. As a best practice, specify a resource using its [Amazon Resource Name \(ARN\)](#). You can do this for actions that support a specific resource type, known as *resource-level permissions*.

For actions that don't support resource-level permissions, such as listing operations, use a wildcard (*) to indicate that the statement applies to all resources.

```
"Resource": "*"
```

To see a list of AWS Audit Manager resource types and their ARNs, see [Resources defined by AWS Audit Manager](#) in the *Service Authorization Reference*. To learn about actions with which you can specify the ARN of each resource, see [Actions defined by AWS Audit Manager](#).

An Audit Manager assessment has the following Amazon Resource Name (ARN) format:

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${assessmentId}
```

An Audit Manager control set has the following ARN format:

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${assessmentId}controlSet/${controlSetId}
```

An Audit Manager control has the following ARN format:

```
arn:${Partition}:auditmanager:${Region}:${Account}:control/${controlId}
```

For more information about the format of ARNs, see [Amazon Resource Names \(ARNs\)](#).

For example, to specify the i-1234567890abcdef0 assessment in your statement, use the following ARN.

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/i-1234567890abcdef0"
```

To specify all instances that belong to a specific account, use the wildcard (*).

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/*"
```

Some Audit Manager actions, such as those for creating resources, cannot be performed on a specific resource. In those cases, you must use the wildcard (*).

```
"Resource": "*"
```

Many Audit Manager API actions involve multiple resources. For example, `ListAssessments` returns a list of assessment metadata that's accessible by the currently logged in AWS account. Therefore, a user must have permissions to view the assessments. To specify multiple resources in a single statement, separate the ARNs with commas.

```
"Resource": [  
    "resource1",  
    "resource2"]
```

To see a list of Audit Manager resource types and their ARNs, see [Resources Defined by AWS Audit Manager](#) in the *IAM User Guide*. To learn about actions with which you can specify the ARN of each resource, see [Actions Defined by AWS Audit Manager](#).

Some Audit Manager API actions support multiple resources. For example, `GetChangeLogs` accesses an `assessmentID`, `controlID`, and `controlSetId`, so a principal must have permissions to access each of these resources. To specify multiple resources in a single statement, separate the ARNs with commas.

```
"Resource": [  
    "assessmentId",  
    "controlId",  
    "controlSetId"]
```

Policy condition keys for AWS Audit Manager

Supports service-specific policy condition keys	Partial
-------------------------------------------------	---------

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The Condition element (or Condition *block*) lets you specify conditions in which a statement is in effect. The Condition element is optional. You can create conditional expressions that use [condition operators](#), such as equals or less than, to match the condition in the policy with values in the request.

If you specify multiple Condition elements in a statement, or multiple keys in a single Condition element, AWS evaluates them using a logical AND operation. If you specify multiple values for a single condition key, AWS evaluates the condition using a logical OR operation. All of the conditions must be met before the statement's permissions are granted.

When the principal in a policy statement is an [AWS service principal](#), we strongly recommend that you use the [aws:SourceArn](#) or [aws:SourceAccount](#) global condition keys in the policy. You can use these global condition context keys to help prevent the [confused deputy scenario](#). The following documented policies show how you can use the aws:SourceArn and aws:SourceAccount global condition context keys in Audit Manager to prevent the confused deputy problem.

- [Example policy for an SNS topic that's used for Audit Manager notifications](#)
- [Example policy for a KMS key that's used with an SNS topic](#)

You can also use placeholder variables when you specify conditions. For example, you can grant a user permission to access a resource only if it is tagged with their user name. For more information, see [IAM policy elements: variables and tags](#) in the *IAM User Guide*.

Audit Manager does not provide any service-specific condition keys, but it does support using some global condition keys. To see all AWS global condition keys, see [AWS global condition context keys](#) in the *IAM User Guide*.

Access control lists (ACLs) in AWS Audit Manager

Supports ACLs	No
---------------	----

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

Attribute-based access control (ABAC) with AWS Audit Manager

Supports ABAC (tags in policies)	Yes
----------------------------------	-----

Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes. In AWS, these attributes are called *tags*. You can attach tags to IAM entities (users or roles) and to many AWS resources. Tagging entities and resources is the first step of ABAC. Then you design ABAC policies to allow operations when the principal's tag matches the tag on the resource that they are trying to access.

ABAC is helpful in environments that are growing rapidly and helps with situations where policy management becomes cumbersome.

To control access based on tags, you provide tag information in the [condition element](#) of a policy using the `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, or `aws:TagKeys` condition keys.

If a service supports all three condition keys for every resource type, then the value is **Yes** for the service. If a service supports all three condition keys for only some resource types, then the value is **Partial**.

For more information about ABAC, see [What is ABAC?](#) in the *IAM User Guide*. To view a tutorial with steps for setting up ABAC, see [Use attribute-based access control \(ABAC\)](#) in the *IAM User Guide*.

For more information about tagging AWS Audit Manager resources, see [Tagging AWS Audit Manager resources \(p. 367\)](#).

Using temporary credentials with AWS Audit Manager

Supports temporary credentials	Yes
--------------------------------	-----

Some AWS services don't work when you sign in using temporary credentials. For additional information, including which AWS services work with temporary credentials, see [AWS services that work with IAM](#) in the *IAM User Guide*.

You are using temporary credentials if you sign in to the AWS Management Console using any method except a user name and password. For example, when you access AWS using your company's single sign-on (SSO) link, that process automatically creates temporary credentials. You also automatically create temporary credentials when you sign in to the console as a user and then switch roles. For more information about switching roles, see [Switching to a role \(console\)](#) in the *IAM User Guide*.

You can manually create temporary credentials using the AWS CLI or AWS API. You can then use those temporary credentials to access AWS. AWS recommends that you dynamically generate temporary credentials instead of using long-term access keys. For more information, see [Temporary security credentials in IAM](#).

Cross-service principal permissions for AWS Audit Manager

Supports principal permissions	Yes
--------------------------------	-----

When you use an IAM user or role to perform actions in AWS, you are considered a principal. Policies grant permissions to a principal. When you use some services, you might perform an action that then triggers another action in a different service. In this case, you must have permissions to perform both actions. To see whether an action requires additional dependent actions in a policy, see [Actions, Resources, and Condition Keys for AWS Audit Manager](#) in the *Service Authorization Reference*.

Service roles for AWS Audit Manager

Supports service roles	No
------------------------	----

A service role is an [IAM role](#) that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see [Creating a role to delegate permissions to an AWS service](#) in the *IAM User Guide*.

Warning

Changing the permissions for a service role might break AWS Audit Manager functionality. Edit service roles only when Audit Manager provides guidance to do so.

Service-linked roles for AWS Audit Manager

Supports service-linked roles	Yes
-------------------------------	-----

A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

For details about service-linked roles for AWS Audit Manager, see [Using service-linked roles for AWS Audit Manager \(p. 351\)](#).

Identity-based policy examples for AWS Audit Manager

By default, users and roles don't have permission to create or modify Audit Manager resources. They also can't perform tasks by using the AWS Management Console, AWS Command Line Interface (AWS CLI), or AWS API. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

To learn how to create an IAM identity-based policy by using these example JSON policy documents, see [Creating IAM policies](#) in the *IAM User Guide*.

For details about actions and resource types defined by AWS Audit Manager, including the format of the ARNs for each of the resource types, see [Actions, resources, and condition keys for AWS Audit Manager](#) in the *Service Authorization Reference*.

Topics

- [Policy best practices \(p. 323\)](#)
- [Allow the minimum permissions required to enable Audit Manager \(p. 324\)](#)
- [Allow users full administrator access to AWS Audit Manager \(p. 325\)](#)
- [Allow users management access to AWS Audit Manager \(p. 331\)](#)
- [Allow users read-only access to AWS Audit Manager \(p. 332\)](#)
- [Allow users to view their own permissions \(p. 333\)](#)
- [Allow AWS Audit Manager to send notifications to Amazon SNS topics \(p. 333\)](#)
- [Allow users to run search queries in evidence finder \(p. 336\)](#)

Policy best practices

Identity-based policies determine whether someone can create, access, or delete Audit Manager resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *AWS managed policies* that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see [AWS managed policies](#) or [AWS managed policies for job functions](#) in the *IAM User Guide*.
- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see [Policies and permissions in IAM](#) in the *IAM User Guide*.
- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all

requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as AWS CloudFormation. For more information, see [IAM JSON policy elements: Condition](#) in the *IAM User Guide*.

- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions**
– IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see [IAM Access Analyzer policy validation](#) in the *IAM User Guide*.
- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or a root user in your AWS account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see [Configuring MFA-protected API access](#) in the *IAM User Guide*.

For more information about best practices in IAM, see [Security best practices in IAM](#) in the *IAM User Guide*.

Allow the minimum permissions required to enable Audit Manager

This example shows how you might allow accounts without an administrator role to enable AWS Audit Manager.

Note

What we provide here is a basic policy that grants the minimum permissions needed to enable Audit Manager. All of the permissions in the following policy are required. If you omit any part of this policy, you won't be able to enable Audit Manager.

We recommend that you take time to customize your permissions so they meet your specific needs. If you need help, contact your administrator or [AWS Support](#).

To grant the minimum access required to enable Audit Manager, use the following permissions.

```
{  
    "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:currentAccount"  
                    ]  
                }  
            }  
        }  
    ]  
}
```

```

        "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"
        }
    }
}
]
}

```

You don't need to allow minimum console permissions for users that are making calls only to the AWS CLI or the AWS API. Instead, allow access to only the actions that match the API operation that you're trying to perform.

Allow users full administrator access to AWS Audit Manager

The following example policies grant full administrator access to AWS Audit Manager.

- [Example 1 \(Managed policy, AWSAuditManagerAdministratorAccess\) \(p. 325\)](#)
- [Example 2 \(Assessment report destination permissions\) \(p. 328\)](#)
- [Example 3 \(Export destination permissions\) \(p. 328\)](#)
- [Example 4 \(Permissions to enable evidence finder\) \(p. 330\)](#)
- [Example 5 \(Permissions to disable evidence finder\) \(p. 330\)](#)

Example 1 (Managed policy, AWSAuditManagerAdministratorAccess)

The policy in this example is the managed policy, `AWSAuditManagerAdministratorAccess`. This policy includes the ability to enable and disable Audit Manager, the ability to change Audit Manager settings, and the ability to manage all Audit Manager resources such as assessments, frameworks, controls, and assessment reports.

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

```

```
"Sid": "OrganizationsAccess",
"Effect": "Allow",
>Action": [
    "organizations>ListAccountsForParent",
    "organizations>ListAccounts",
    "organizations>DescribeOrganization",
    "organizations>DescribeOrganizationalUnit",
    "organizations>DescribeAccount",
    "organizations>ListParents",
    "organizations>ListChildren"
],
"Resource": "*"
},
{
"Sid": "AllowOnlyAuditManagerIntegration",
"Effect": "Allow",
>Action": [
    "organizations:RegisterDelegatedAdministrator",
    "organizations>DeregisterDelegatedAdministrator",
    "organizations>EnableAWSAccess"
],
"Resource": "*",
"Condition": {
    "StringLikeIfExists": {
        "organizations>ServicePrincipal": [
            "auditmanager.amazonaws.com"
        ]
    }
}
},
{
"Sid": "IAMAccess",
"Effect": "Allow",
>Action": [
    "iam>GetUser",
    "iam>ListUsers",
    "iam>ListRoles"
],
"Resource": "*"
},
{
"Sid": "IAMAccessCreateSLR",
"Effect": "Allow",
>Action": "iam>CreateServiceLinkedRole",
"Resource": "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
"Condition": {
    "StringLike": {
        "iam:AWSServiceName": "auditmanager.amazonaws.com"
    }
}
},
{
"Sid": "IAMAccessManageSLR",
"Effect": "Allow",
>Action": [
    "iam>DeleteServiceLinkedRole",
    "iam>UpdateRoleDescription",
    "iam>GetServiceLinkedRoleDeletionStatus"
],
"Resource": "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*"
},
{
"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": "CreateEventsAccess",
    "Effect": "Allow",
    "Action": [
        "events>PutRule"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "events:detail-type": "Security Hub Findings - Imported"
        },
        "ForAllValues:StringEquals": {
            "events:source": [
                "aws.securityhub"
            ]
        }
    }
},
{
    "Sid": "EventsAccess",
    "Effect": "Allow",
    "Action": [
        "events>DeleteRule",
        "events>DescribeRule",
        "events>EnableRule",
        "events>DisableRule",
        "events>ListTargetsByRule",

```

```

        "events:PutTargets",
        "events:RemoveTargets"
    ],
    "Resource": "arn:aws:events:*::rule/AuditManagerSecurityHubFindingsReceiver"
},
{
    "Sid": "TagAccess",
    "Effect": "Allow",
    "Action": [
        "tag:GetResources"
    ],
    "Resource": "*"
}
]
}

```

Example 2 (Assessment report destination permissions)

This policy grants you permission to access a specific S3 bucket, and to add files to and delete files from it. This allows you to use the specified bucket as an assessment report destination in Audit Manager.

Replace the *placeholder text* with your own information. Include the S3 bucket that you use as your assessment report destination and the KMS key that you use to encrypt your assessment reports.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3>ListBucket",
                "s3>DeleteObject",
                "s3:GetBucketLocation",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
        }
    ]
},
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}

```

Example 3 (Export destination permissions)

The following policy allows CloudTrail to deliver evidence finder query results to the specified S3 bucket. As a security best practice, the IAM global condition key `aws:SourceArn` helps ensure that CloudTrail writes to the S3 bucket only for the event data store.

Replace the *placeholder text* with your own information, as follows:

- Replace *DOC-EXAMPLE-DESTINATION-BUCKET* with the S3 bucket that you use as your export destination.
- Replace *myQueryRunningRegion* with the appropriate AWS Region for your configuration.
- Replace *myAccountID* with the AWS account ID that's used for CloudTrail. This might not be the same as the AWS account ID for the S3 bucket. If this is an organization event data store, you must use the AWS account for the management account.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "cloudtrail.amazonaws.com"  
            },  
            "Action": [  
                "s3:PutObject*",  
                "s3:Abort*"  
            ],  
            "Resource": [  
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",  
                "arn:aws:s3:::DOC-EXAMPLE-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:::DOC-EXAMPLE-DESTINATION-BUCKET",  
            "Condition": {  
                "StringEquals": {  
                    "AWS:SourceArn":  
                        "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "cloudtrail.amazonaws.com"  
            },  
            "Action": [  
                "kms:Decrypt*",  
                "kms:GenerateDataKey*"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "s3.amazonaws.com"  
            },  
            "Action": "DOC-EXAMPLE-DESTINATION-BUCKET/*"  
        }  
    ]  
}
```

```
        "Action": [
            "kms:Decrypt*",
            "kms:GenerateDataKey*"
        ],
        "Resource": "*"
    }
}
```

Example 4 (Permissions to enable evidence finder)

The following permission policy is required if you want to enable and use the evidence finder feature. This policy statement allows Audit Manager to create a CloudTrail Lake event data store and run search queries.

```
{
    "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/*"
        }
    ]
}
```

Example 5 (Permissions to disable evidence finder)

This example policy grants permission to disable the evidence finder feature in Audit Manager. This involves deleting the event data store that was created when you first enabled the feature.

Before you use this policy, replace the *placeholder text* with your own information. You should specify the UUID of the event data store that was created when you enabled evidence finder. You can retrieve the ARN of the event data store from your Audit Manager settings. For more information, see [GetSettings](#) in the *AWS Audit Manager API Reference*.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail>DeleteEventDataStore",
                "cloudtrail>UpdateEventDataStore"
            ],
            "Resource": "arn:aws:cloudtrail:::event-data-store-UUID"
        }
    ]
}
```

```
    ]  
}
```

Allow users management access to AWS Audit Manager

This example shows how you might allow non-administrator management access to AWS Audit Manager.

This policy grants the ability to manage all Audit Manager resources (assessments, frameworks, and controls), but does not grant the ability to enable or disable Audit Manager or to modify Audit Manager settings.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AuditManagerAccess",  
            "Effect": "Allow",  
            "Action": [  
                "auditmanager:GetAccountStatus",  
                "auditmanager>ListAssessmentFrameworks",  
                "auditmanager>CreateAssessmentFramework",  
                "auditmanager:GetAssessmentFramework",  
                "auditmanager:UpdateAssessmentFramework",  
                "auditmanager>DeleteAssessmentFramework",  
                "auditmanager>ListAssessmentReports",  
                "auditmanager>ListAssessments",  
                "auditmanager>CreateAssessment",  
                "auditmanager>ListControls",  
                "auditmanager>CreateControl",  
                "auditmanager>GetControl",  
                "auditmanager:UpdateControl",  
                "auditmanager>DeleteControl",  
                "auditmanager>ListKeywordsForDataSource",  
                "auditmanager>GetDelegations",  
                "auditmanager>ValidateAssessmentReportIntegrity",  
                "auditmanager>ListNotifications",  
                "auditmanager>GetServicesInScope",  
                "auditmanager>GetSettings",  
                "auditmanager>ListTagsForResource",  
                "auditmanager>TagResource",  
                "auditmanager>UntagResource"  
            ],  
            "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": "SNSSAccess",
    "Effect": "Allow",
    "Action": [
        "sns>ListTopics"
    ],
    "Resource": "*"
},
{
    "Sid": "TagAccess",
    "Effect": "Allow",
    "Action": [
        "tag>GetResources"
    ],
    "Resource": "*"
}
]
```

Allow users read-only access to AWS Audit Manager

This policy grants read-only access to AWS Audit Manager resources such as assessments, frameworks, and controls.

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

Allow users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```
{  
    "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": "*"  
        }  
    ]  
}
```

Allow AWS Audit Manager to send notifications to Amazon SNS topics

The policies in this example grant Audit Manager permissions to send notifications to an existing Amazon SNS topic.

- [Example 1](#) – If you want to receive notifications from Audit Manager, use this example to add permissions to your SNS topic access policy.
- [Example 2](#) – If your SNS topic uses AWS Key Management Service (AWS KMS) for server-side encryption (SSE), use this example to add permissions to the KMS key access policy.

In the following policies, the principal who gets the permissions is the Audit Manager service principal, which is `auditmanager.amazonaws.com`. When the principal in a policy statement is an [AWS service principal](#), we strongly recommend that you use the `aws:SourceArn` or `aws:SourceAccount` global condition keys in the policy. You can use these global condition context keys to help prevent the [confused deputy scenario](#).

Example 1 (Permissions for the SNS topic)

This policy statement allows Audit Manager to publish events to the specified SNS topic. Any request to publish to the specified SNS topic must satisfy the policy conditions.

Before using this policy, replace the *placeholder text* with your own information. Take note of the following:

- If you use the `aws:SourceArn` condition key in this policy, the value must be the ARN of the Audit Manager resource that the notification comes from. In the example below, `aws:SourceArn` uses a wildcard (*) for the resource ID. This allows all requests that come from Audit Manager on all Audit Manager resources. With the `aws:SourceArn` global condition key, you can use either the `StringLike` or the `ArnLike` condition operator. As a best practice, we recommend that you use `ArnLike`.
- If you use the `aws:SourceAccount` condition key, you can use either the `StringEquals` or the `StringLike` condition operator. As a best practice, we recommend that you use `StringEquals` to implement least privilege.
- If you use both `aws:SourceAccount` and `aws:SourceArn`, the account values must show the same account ID.

```
{  
    "Version": "2012-10-17",  
    "Statement": {  
        "Sid": "AllowAuditManagerToUseSNSTopic",  
        "Effect": "Allow",  
        "Principal": {  
            "Service": "auditmanager.amazonaws.com"  
        },  
        "Action": "SNS:Publish",  
        "Resource": "arn:aws:sns:region:accountID:topicName",  
        "Condition": {  
            "StringEquals": {  
                "aws:SourceAccount": "accountID"  
            },  
            "ArnLike": {  
                "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"  
            }  
        }  
    }  
}
```

The following alternative example uses just the `aws:SourceArn` condition key, with the `StringLike` condition operator:

```
"Condition": {  
    "StringLike": {  
        "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"  
    }  
}
```

The following alternative example uses just the `aws:SourceAccount` condition key, with the `StringLike` condition operator:

```
"Condition": {  
    "StringLike": {  
        "aws:SourceAccount": "accountID"  
    }  
}
```

Example 2 (Permissions for the KMS key that's attached to the SNS topic)

This policy statement allows Audit Manager to use the KMS key to [generate the data key](#) that it uses to encrypt an SNS topic. Any request to use the KMS key for the specified operation must satisfy the policy conditions.

Before using this policy, replace the *placeholder text* with your own information. Take note of the following:

- If you use the `aws:SourceArn` condition key in this policy, the value must be the ARN of the resource that's being encrypted. For example, in this case, it's the SNS topic in your account. Set the value to the ARN or an ARN pattern with wildcard characters (*). You can use either the `StringLike` or the `ArnLike` condition operator with the `aws:SourceArn` condition key. As a best practice, we recommend that you use `ArnLike`.
- If you use the `aws:SourceAccount` condition key, you can use either the `StringEquals` or the `StringLike` condition operator. As a best practice, we recommend that you use `StringEquals` to implement least privilege. You can use `aws:SourceAccount` if you don't know the ARN of the SNS topic.
- If you use both `aws:SourceAccount` and `aws:SourceArn`, the account values must show the same account ID.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowAuditManagerToUseKMSKey",  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "auditmanager.amazonaws.com"  
            },  
            "Action": [  
                "kms:Decrypt",  
                "kms:GenerateDataKey"  
            ],  
            "Resource": "arn:aws:kms:region:accountID:key/*",  
            "Condition": {  
                "StringEquals": {  
                    "aws:SourceAccount": "accountID"  
                }  
                "ArnLike": {  
                    "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"  
                }  
            }  
        }  
    ]  
}
```

The following alternative example uses just the `aws:SourceArn` condition key, with the `StringLike` condition operator:

```
"Condition": {  
    "StringLike": {  
        "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"  
    }  
}
```

The following alternative example uses just the `aws:SourceAccount` condition key, with the `StringLike` condition operator:

```
"Condition": {
```

```
    "StringLike": {
        "aws:SourceAccount": "accountID"
    }
}
```

Allow users to run search queries in evidence finder

The following policy grants permissions to perform queries on a CloudTrail Lake event data store. This permission policy is required if you want to use the evidence finder feature.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageCloudTrailLakeQueryAccess",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:StartQuery",
                "cloudtrail:DescribeQuery",
                "cloudtrail:GetQueryResults",
                "cloudtrail:CancelQuery"
            ],
            "Resource": "*"
        }
    ]
}
```

Cross-service confused deputy prevention

The confused deputy problem is a security issue where an entity that doesn't have permission to perform an action can coerce a more-privileged entity to perform the action. In AWS, cross-service impersonation can result in the confused deputy problem. Cross-service impersonation can occur when one service (the *calling service*) calls another service (the *called service*). The calling service can be manipulated to use its permissions to act on another customer's resources when it doesn't have permission to do so. To prevent this, Amazon Web Services provides tools that help you protect your data for all services with service principals that have been given access to resources in your account.

We recommend using the [aws:SourceArn](#) and [aws:SourceAccount](#) global condition context keys in resource policies to limit the permissions that AWS Audit Manager gives to another service for access to your resources.

- Use [aws:SourceArn](#) if you want only one resource to be associated with the cross-service access. You can also use [aws:SourceArn](#) with a wildcard (*) if you want to specify multiple resources.

For example, you might use an Amazon SNS topic to receive activity notifications from Audit Manager. In this case, in your SNS topic access policy, the ARN value of [aws:SourceArn](#) is the Audit Manager resource that the notification comes from. Because it's likely that you have multiple Audit Manager resources, we recommend that you use [aws:SourceArn](#) with a wildcard. This enables you to specify all of your Audit Manager resources in your SNS topic access policy.

- Use [aws:SourceAccount](#) if you want to allow any resource in that account to be associated with the cross-service use.
- If the [aws:SourceArn](#) value doesn't contain the account ID, such as an Amazon S3 bucket ARN, you must use both global condition context keys to limit permissions.
- If you use both conditions, and if the [aws:SourceArn](#) value contains the account ID, the [aws:SourceAccount](#) value and the account in the [aws:SourceArn](#) value must show the same account ID when used in the same policy statement.

- The most effective way to protect against the confused deputy problem is to use the aws:SourceArn global condition context key with the full ARN of the resource. If you don't know the full Amazon Resource Name (ARN) of the resource or if you are specifying multiple resources, use the aws:SourceArn global context condition key with wildcard characters (*) for the unknown portions of the ARN. For example, arn:aws:servicename:*:123456789012:*.

Audit Manager confused deputy support

Audit Manager provides confused deputy support in the following scenarios. These policy examples show how you can use the aws:SourceArn and aws:SourceAccount condition keys to prevent the confused deputy problem.

- [Example policy: The SNS topic that you use to receive Audit Manager notifications](#)
- [Example policy: The KMS key that you use to encrypt your SNS topic](#)

Audit Manager doesn't provide confused deputy support for the customer managed key that you provide in your Audit Manager [Data encryption \(p. 252\)](#) settings. If you provided your own customer managed key, you can't use aws:SourceAccount or aws:SourceArn conditions in that KMS key policy.

AWS managed policies for AWS Audit Manager

An AWS managed policy is a standalone policy that is created and administered by AWS. AWS managed policies are designed to provide permissions for many common use cases so that you can start assigning permissions to users, groups, and roles.

Keep in mind that AWS managed policies might not grant least-privilege permissions for your specific use cases because they're available for all AWS customers to use. We recommend that you reduce permissions further by defining [customer managed policies](#) that are specific to your use cases.

You cannot change the permissions defined in AWS managed policies. If AWS updates the permissions defined in an AWS managed policy, the update affects all principal identities (users, groups, and roles) that the policy is attached to. AWS is most likely to update an AWS managed policy when a new AWS service is launched or new API operations become available for existing services.

For more information, see [AWS managed policies](#) in the *IAM User Guide*.

Topics

- [AWS managed policy: AWSAuditManagerAdministratorAccess \(p. 337\)](#)
- [AWS managed policy: AWSAuditManagerServiceRolePolicy \(p. 341\)](#)
- [AWS Audit Manager updates to AWS managed policies \(p. 347\)](#)

AWS managed policy: AWSAuditManagerAdministratorAccess

You can attach the AWSAuditManagerAdministratorAccess policy to your IAM identities.

This policy grants administrative permissions that allow full administration access to AWS Audit Manager. This access includes the ability to enable and disable AWS Audit Manager, change settings in AWS Audit Manager, and manage all Audit Manager resources such as assessments, frameworks, controls, and assessment reports.

AWS Audit Manager requires broad permissions across multiple AWS services. This is because AWS Audit Manager integrates with multiple AWS services to collect evidence automatically from the AWS account and services in scope of an assessment.

Permissions details

This policy includes the following permissions:

- **Audit Manager** – Allows principals full permissions on AWS Audit Manager resources.
- **Organizations** – Allows principals to list accounts and organizational units, and to register or deregister a delegated administrator. This is required so that you can enable multi-account support and allow AWS Audit Manager to run assessments over multiple accounts and consolidate evidence into a delegated administrator account.
- **iam** – Allows principals to get and list users in IAM and create a service-linked role. This is required so that you can designate audit owners and delegates for an assessment. This policy also allows principals to delete the service-linked role and retrieve the deletion status. This is required so that AWS Audit Manager can clean up resources and delete the service-linked role for you when you choose to disable the service in the AWS Management Console.
- **s3** – Allows principals to list available Amazon Simple Storage Service (Amazon S3) buckets. This capability is required so that you can designate the S3 bucket in which you want to store evidence reports or upload manual evidence.
- **kms** – Allows principals to list and describe keys, list aliases, and create grants. This is required so that you can choose customer managed keys for data encryption.
- **sns** – Allows principals to list subscription topics in Amazon SNS. This is required so that you can specify which SNS topic you want AWS Audit Manager to send notifications to.
- **events** – Allows principals to list and manage checks from AWS Security Hub. This is required so that AWS Audit Manager can automatically collect AWS Security Hub findings for the AWS services that are monitored by AWS Security Hub. It can then convert this data into evidence to be included in your AWS Audit Manager assessments.
- **tag** – Allows principals to retrieve tagged resources. This is required so that you can use tags as a search filter when browsing frameworks, controls, and assessments in AWS Audit Manager.

```
{  
    "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": "AllowOnlyAuditManagerIntegration",  
            "Effect": "Allow",  
            "Action": [  
                "organizations>RegisterDelegatedAdministrator",  
                "organizations>DeregisterDelegatedAdministrator",  
                "organizations>EnableAWSAccess"  
            ]  
        }  
    ]  
}
```

```
        ],
        "Resource": "*",
        "Condition": {
            "StringLikeIfExists": {
                "organizations:ServicePrincipal": [
                    "auditmanager.amazonaws.com"
                ]
            }
        }
    },
    {
        "Sid": "IAMAccess",
        "Effect": "Allow",
        "Action": [
            "iam:GetUser",
            "iam>ListUsers",
            "iam>ListRoles"
        ],
        "Resource": "*"
    },
    {
        "Sid": "IAMAccessCreateSLR",
        "Effect": "Allow",
        "Action": "iam>CreateServiceLinkedRole",
        "Resource": "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/AWSServiceRoleForAuditManager",
        "Condition": {
            "StringLike": {
                "iam:AWSServiceName": "auditmanager.amazonaws.com"
            }
        }
    },
    {
        "Sid": "IAMAccessManageSLR",
        "Effect": "Allow",
        "Action": [
            "iam>DeleteServiceLinkedRole",
            "iam>UpdateRoleDescription",
            "iam:GetServiceLinkedRoleDeletionStatus"
        ],
        "Resource": "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/AWSServiceRoleForAuditManager"
    },
    {
        "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": "CreateEventsAccess",
        "Effect": "Allow",
        "Action": [
            "events:PutRule"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "events:detail-type": "Security Hub Findings - Imported"
            },
            "ForAllValues:StringEquals": {
                "events:source": [
                    "aws.securityhub"
                ]
            }
        }
    },
    {
        "Sid": "EventsAccess",
        "Effect": "Allow",
        "Action": [
            "events>DeleteRule",
            "events:DescribeRule",
            "events:EnableRule",
            "events:DisableRule",
            "events>ListTargetsByRule",
            "events:PutTargets",
            "events:RemoveTargets"
        ],
        "Resource": "arn:aws:events:*::rule/AuditManagerSecurityHubFindingsReceiver"
    },
    {
        "Sid": "TagAccess",
        "Effect": "Allow",
        "Action": [
            "tag:GetResources"
        ],
        "Resource": "*"
    }
]
```

AWS managed policy: AWSAuditManagerServiceRolePolicy

You can't attach `AWSAuditManagerServiceRolePolicy` to your IAM entities. This policy is attached to a service-linked role, `AWSServiceRoleForAuditManager`, that allows AWS Audit Manager to perform actions on your behalf. For more information, see [Using service-linked roles for AWS Audit Manager](#).

The role permissions policy, `AWSAuditManagerServiceRolePolicy`, allows AWS Audit Manager to collect automated evidence by doing the following on your behalf:

- Collect data from the following data sources:
 - Management events from AWS CloudTrail
 - Compliance checks from AWS Config Rules
 - Compliance checks from AWS Security Hub
- Use API calls to describe your resource configurations for the following AWS services.

Tip

For more information about the API calls that Audit Manager uses to collect evidence from these services, see [Supported API calls for custom control data sources \(p. 247\)](#) in this guide.

- AWS Certificate Manager
- AWS Backup
- Amazon Bedrock
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch Logs
- Amazon Cognito user pools
- AWS Config
- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2
- Amazon Elastic Container Service
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Amazon ElastiCache
- Elastic Load Balancing
- Amazon EMR
- Amazon EventBridge
- Amazon Kinesis Data Firehose
- Amazon FSx
- Amazon GuardDuty
- AWS Identity and Access Management (IAM)
- Amazon Kinesis
- AWS KMS
- AWS Lambda
- AWS License Manager
- Amazon Managed Streaming for Apache Kafka
- AWS Organizations
- Amazon Relational Database Service
- Amazon Redshift

- Amazon Route 53
- Amazon S3
- AWS Security Hub
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- AWS WAF

Permissions details

`AWSAuditManagerServiceRolePolicy` allows AWS Audit Manager to complete the following actions on the specified resources:

- `acm:GetAccountConfiguration`
- `acm>ListCertificates`
- `backup>ListRecoveryPointsByResource`
- `bedrock:GetCustomModel`
- `bedrock:GetFoundationModel`
- `bedrock:GetModelCustomizationJob`
- `bedrock:GetModelInvocationLoggingConfiguration`
- `bedrock>ListCustomModels`
- `bedrock>ListFoundationModels`
- `bedrock>ListModelCustomizationJobs`
- `cloudtrail:DescribeTrails`
- `cloudtrail:LookupEvents`
- `cloudwatch:DescribeAlarms`
- `cloudwatch:DescribeAlarmsForMetric`
- `cloudwatch:GetMetricStatistics`
- `cloudwatch>ListMetrics`
- `cognito-idp:DescribeUserPool`
- `config:DescribeConfigRules`
- `config:DescribeDeliveryChannels`
- `config>ListDiscoveredResources`
- `directconnect:DescribeDirectConnectGateways`
- `directconnect:DescribeVirtualGateways`
- `dynamodb:DescribeTable`
- `dynamodb>ListBackups`
- `dynamodb>ListGlobalTables`
- `dynamodb>ListTables`
- `ec2:DescribeAddresses`
- `ec2:DescribeCustomerGateways`
- `ec2:DescribeEgressOnlyInternetGateways`
- `ec2:DescribeFlowLogs`
- `ec2:DescribeInstances`
- `ec2:DescribeInternetGateways`
- `ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations`
- `ec2:DescribeLocalGateways`

- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce>ListClusters
- elasticmapreduce>ListSecurityConfigurations
- 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:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy

- iam:GetAccountSummary
- iam:GetCredentialReport
- iam>ListEntitiesForPolicy
- iam>ListGroupPolicies
- iam>ListGroups
- iam>ListOpenIdConnectProviders
- iam>ListPolicies
- 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
- organizations>DescribeOrganization
- organizations>DescribePolicy
- rds>DescribeCertificates
- rds>DescribeDbClusterEndpoints
- rds>DescribeDbClusterParameterGroups
- rds>DescribeDbClusters
- rds>DescribeDBInstances
- rds>DescribeDbSecurityGroups
- redshift>DescribeClusters
- route53>GetQueryLoggingConfig
- s3>GetBucketPublicAccessBlock
- s3>GetBucketVersioning
- s3>GetEncryptionConfiguration

- s3:GetLifecycleConfiguration
 - s3>ListAllMyBuckets
 - securityhub:DescribeStandards
 - sns>ListTopics
 - sqs>ListQueues
 - waf-regional:GetLoggingConfiguration
 - waf-regional>ListRuleGroups
 - waf-regional>ListSubscribedRuleGroups
 - waf-regional>ListWebACLs
 - waf>ListActivatedRulesInRuleGroup

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "acm:GetAccountConfiguration",  
        "acm>ListCertificates",  
        "backup>ListRecoveryPointsByResource",  
        "bedrock:GetCustomModel",  
        "bedrock:GetFoundationModel",  
        "bedrock:GetModelCustomizationJob",  
        "bedrock:GetModelInvocationLoggingConfiguration",  
        "bedrock>ListCustomModels",  
        "bedrock>ListFoundationModels",  
        "bedrock>ListModelCustomizationJobs",  
        "cloudtrail:DescribeTrails",  
        "cloudtrail:LookupEvents",  
        "cloudwatch:DescribeAlarms",  
        "cloudwatch:DescribeAlarmsForMetric",  
        "cloudwatch:GetMetricStatistics",  
        "cloudwatch>ListMetrics",  
        "cognito-identity:DescribeUserPool",  
        "config:DescribeConfigRules",  
        "config:DescribeDeliveryChannels",  
        "config>ListDiscoveredResources",  
        "directconnect:DescribeDirectConnectGateways",  
        "directconnect:DescribeVirtualGateways",  
        "dynamodb:DescribeTable",  
        "dynamodb>ListBackups",  
        "dynamodb>ListGlobalTables",  
        "dynamodb>ListTables",  
        "ec2:DescribeAddresses",  
        "ec2:DescribeCustomerGateways",  
        "ec2:DescribeEgressOnlyInternetGateways",  
        "ec2:DescribeFlowLogs",  
        "ec2:DescribeInstances",  
        "ec2:DescribeInternetGateways",  
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",  
        "ec2:DescribeLocalGateways",  
        "ec2:DescribeLocalGatewayVirtualInterfaces",  
        "ec2:DescribeNatGateways",  
        "ec2:DescribeNetworkAcls",  
        "ec2:DescribeRouteTables",  
        "ec2:DescribeSecurityGroups",  
        "ec2:DescribeSnapshots",  
        "ec2:DescribeTransitGateways",  
        "ec2:DescribeVolumes",  
        "ec2:DescribeVpcEndpoints".  
      ]  
    }  
  ]  
}
```

```
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeVpcs",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:GetEbsDefaultKmsKeyId",
"ec2:GetEbsEncryptionByDefault",
"ecs:DescribeClusters",
"eks:DescribeAddonVersions",
"elasticache:DescribeCacheClusters",
"elasticache:DescribeServiceUpdates",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeFileSystems",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeSslPolicies",
"elasticloadbalancing:DescribeTargetGroups",
"elasticmapreduce>ListClusters",
"elasticmapreduce>ListSecurityConfigurations",
"events:DescribeRule",
"events>ListConnections",
"events>ListEventBuses",
"events>ListEventSources",
"events>ListRules",
"firehose>ListDeliveryStreams",
"fsx:DescribeFileSystems",
"guardduty>ListDetectors",
"iam:GenerateCredentialReport",
"iam:GetAccountAuthorizationDetails",
"iam:GetAccountPasswordPolicy",
"iam:GetAccountSummary",
"iam:GetCredentialReport",
"iam>ListEntitiesForPolicy",
"iam>ListGroupPolicies",
"iam>ListGroups",
"iam>ListOpenIdConnectProviders",
"iam>ListPolicies",
"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",
"organizations:DescribeOrganization",
"organizations:DescribePolicy",
"rds:DescribeCertificates",
"rds:DescribeDbClusterEndpoints",
"rds:DescribeDbClusterParameterGroups",
"rds:DescribeDbClusters",
```

```
"rds:DescribeDBInstances",
"rds:DescribeDbSecurityGroups",
"redshift:DescribeClusters",
"route53:GetQueryLoggingConfig",
"s3:GetBucketPublicAccessBlock",
"s3:GetBucketVersioning",
"s3:GetEncryptionConfiguration",
"s3:GetLifecycleConfiguration",
"s3>ListAllMyBuckets",
"securityhub:DescribeStandards",
"sns>ListTopics",
"sqs>ListQueues",
"waf-regional:GetLoggingConfiguration",
"waf-regional>ListRuleGroups",
"waf-regional>ListSubscribedRuleGroups",
"waf-regional>ListWebACLS",
"waf>ListActivatedRulesInRuleGroup"
],
"Resource": "*",
"Sid": "s2sAPIsAccess"
},
{
"Sid": "CreateEventsAccess",
"Effect": "Allow",
>Action": [
"events:PutRule"
],
"Resource": "arn:aws:events:*::rule/AuditManagerSecurityHubFindingsReceiver",
"Condition": {
"StringEquals": {
"events:detail-type": "Security Hub Findings - Imported"
},
"Null": {
"events:source": "false"
},
"ForAllValues:StringEquals": {
"events:source": [
"aws.securityhub"
]
}
},
{
"Sid": "EventsAccess",
"Effect": "Allow",
>Action": [
"events>DeleteRule",
"events:DescribeRule",
"events:EnableRule",
"events:DisableRule",
"events>ListTargetsByRule",
"events:PutTargets",
"events:RemoveTargets"
],
"Resource": "arn:aws:events:*::rule/AuditManagerSecurityHubFindingsReceiver"
}
]
```

AWS Audit Manager updates to AWS managed policies

View details about updates to AWS managed policies for AWS Audit Manager since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the AWS Audit Manager [Document history](#) page.

Change	Description	Date
<p><u>AWSAuditManagerServiceRolePolicy</u></p> <ul style="list-style-type: none"> – Update to an existing policy 	<p>We added the following permissions to <code>AWSAuditManagerServiceRolePolicy</code>. AWS Audit Manager can now perform the following actions to collect automated evidence about the resources in your AWS account.</p> <ul style="list-style-type: none"> • <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> • <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> 	11/06/2023

Change	Description	Date
	<ul style="list-style-type: none"> • elasticloadbalancing:DescribeSslPolicies • 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 • rds:DescribeDbClusterParameterGroups • rds:DescribeDbClusters • rds:DescribeDbSecurityGroups • redshift:DescribeClusters • s3:GetBucketPublicAccessBlock • s3:GetBucketVersioning • sns>ListTopics • sqs>ListQueues • waf-regional:GetLoggingConfiguration • waf-regional>ListRuleGroups • waf-regional>ListSubscribedRuleGroups • waf-regional>ListWebACLs 	

Change	Description	Date
<u>AWSAuditManagerServiceRolePolicy</u> – Update to an existing policy	We added the following permissions to AWSAuditManagerServiceRolePolicy: <ul style="list-style-type: none">• dynamodb:DescribeTable• dynamodb>ListTables• ec2:DescribeVolumes• kms:GetKeyPolicy• kms:GetKeyRotationStatus• kms>ListKeyPolicies• rds:DescribeDBInstances• redshift:DescribeClusters• s3:GetEncryptionConfiguration• s3>ListAllMyBuckets	07/07/2022
<u>AWSAuditManagerServiceRolePolicy</u> – Update to an existing policy	The service-linked role now allows AWS Audit Manager to perform the organizations:DescribeOrganization action. We also scoped down the CreateEventsAccess resource from a wildcard (*) to a specific type of resource (arn:aws:events:/*:*:rule/AuditManagerSecurityHubFindingsReceiver). Lastly, we added a Null condition operator for the events:source condition key to confirm that a source value exists and its value is not null.	05/20/2022
<u>AWSAuditManagerAdministratorAccess</u> – Update to an existing policy	We updated the key condition policy for events:source to reflect that this is a multi-valued key.	04/29/2022
<u>AWSAuditManagerServiceRolePolicy</u> – Update to an existing policy	We updated the key condition policy for events:source to reflect that this is a multi-valued key.	03/16/2022
AWS Audit Manager started tracking changes	AWS Audit Manager started tracking changes for its AWS managed policies.	05/06/2021

Troubleshooting AWS Audit Manager identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with Audit Manager and IAM.

Topics

- [I am not authorized to perform an action in AWS Audit Manager \(p. 351\)](#)
- [I am not authorized to perform iam:PassRole \(p. 351\)](#)
- [I want to allow people outside of my AWS account to access my AWS Audit Manager resources \(p. 351\)](#)

I am not authorized to perform an action in AWS Audit Manager

The `AccessDeniedException` error appears when a user doesn't have permission to use AWS Audit Manager or the Audit Manager API operations.

In this case, your administrator must update the policy to allow you access.

I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, your policies must be updated to allow you to pass a role to Audit Manager.

Some AWS services allow you to pass an existing role to that service instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the console to perform an action in Audit Manager. However, the action requires the service to have permissions that are granted by a service role. Mary does not have permissions to pass the role to the service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

In this case, Mary's policies must be updated to allow her to perform the `iam:PassRole` action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

I want to allow people outside of my AWS account to access my AWS Audit Manager resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Audit Manager supports these features, see [How AWS Audit Manager works with IAM \(p. 316\)](#).
- To learn how to provide access to your resources across AWS accounts that you own, see [Providing access to an IAM user in another AWS account that you own](#) in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see [Providing access to AWS accounts owned by third parties](#) in the *IAM User Guide*.
- To learn how to provide access through identity federation, see [Providing access to externally authenticated users \(identity federation\)](#) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see [How IAM roles differ from resource-based policies](#) in the *IAM User Guide*.

Using service-linked roles for AWS Audit Manager

AWS Audit Manager uses AWS Identity and Access Management (IAM) [service-linked roles](#). A service-linked role is a unique type of IAM role that is linked directly to Audit Manager. Service-linked roles are predefined by Audit Manager and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up AWS Audit Manager easier because you don't have to manually add the necessary permissions. Audit Manager defines the permissions of its service-linked roles, and

unless defined otherwise, only Audit Manager can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

For information about other services that support service-linked roles, see [AWS services that work with IAM](#) and look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for AWS Audit Manager

Audit Manager uses the service-linked role named **AWSServiceRoleForAuditManager**, which enables access to AWS services and resources used or managed by AWS Audit Manager.

The **AWSServiceRoleForAuditManager** service-linked role trusts the `auditmanager.amazonaws.com` service to assume the role.

The role permissions policy, [AWSAuditManagerServiceRolePolicy](#), allows Audit Manager to collect automated evidence about your AWS usage. More specifically, it can take the following actions on your behalf.

- Audit Manager can use AWS Security Hub to collect **compliance check** evidence. In this case, Audit Manager uses the following permission to report the results of security checks directly from AWS Security Hub. It then attaches the results to your relevant assessment controls as evidence.
 - `securityhub:DescribeStandards`

Note

For more information about which specific Security Hub controls Audit Manager can describe, see [AWS Security Hub controls supported by AWS Audit Manager](#).

- Audit Manager can use AWS Config to collect **compliance check** evidence. In this case, Audit Manager uses the following permissions to report the results of AWS Config rule evaluations directly from AWS Config. It then attaches the results to your relevant assessment controls as evidence.
 - `config:DescribeConfigRules`
 - `config:DescribeDeliveryChannels`
 - `config>ListDiscoveredResources`

Note

For more information about which specific AWS Config rules Audit Manager can describe, see [AWS Config Rules supported by AWS Audit Manager](#).

- Audit Manager can use AWS CloudTrail to collect **user activity** evidence. In this case, Audit Manager uses the following permissions to capture user activity from CloudTrail logs. It then attaches the activity to your relevant assessment controls as evidence.
 - `cloudtrail:DescribeTrails`
 - `cloudtrail:LookupEvents`

Note

For more information about which specific CloudTrail events Audit Manager can describe, see [AWS CloudTrail event names supported by AWS Audit Manager](#).

- Audit Manager can use AWS API calls to collect **resource configuration** evidence. In this case, Audit Manager uses the following permissions to call read-only APIs that describe your resource configurations for the following AWS services. It then attaches the API responses to your relevant assessment controls as evidence.
 - `acm:GetAccountConfiguration`
 - `acm>ListCertificates`
 - `backup>ListRecoveryPointsByResource`
 - `bedrock:GetCustomModel`
 - `bedrock:GetFoundationModel`

- bedrock:GetModelCustomizationJob
 - bedrock:GetModelInvocationLoggingConfiguration
 - bedrock>ListCustomModels
 - bedrock>ListFoundationModels
 - bedrock>ListModelCustomizationJobs
 - cloudwatch:DescribeAlarms
 - cloudwatch:DescribeAlarmsForMetric
 - cloudwatch:GetMetricStatistics
 - cloudwatch>ListMetrics
 - cognito-idp:DescribeUserPool
 - directconnect:DescribeDirectConnectGateways
 - directconnect:DescribeVirtualGateways
 - dynamodb:DescribeTable
 - dynamodb>ListBackups
 - dynamodb>ListGlobalTables
 - dynamodb>ListTables
 - ec2:DescribeAddresses
 - ec2:DescribeCustomerGateways
 - ec2:DescribeEgressOnlyInternetGateways
 - ec2:DescribeFlowLogs
 - ec2:DescribeInstances
 - ec2:DescribeInternetGateways
 - ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
 - ec2:DescribeLocalGateways
 - ec2:DescribeLocalGatewayVirtualInterfaces
 - ec2:DescribeNatGateways
 - ec2:DescribeNetworkAcls
 - ec2:DescribeRouteTables
 - ec2:DescribeSecurityGroups
 - ec2:DescribeSnapshots
 - ec2:DescribeTransitGateways
 - ec2:DescribeVolumes
 - ec2:DescribeVpcEndpoints
 - ec2:DescribeVpcPeeringConnections
 - ec2:DescribeVpcs
 - ec2:DescribeVpnConnections
 - ec2:DescribeVpnGateways
 - ec2:GetEbsDefaultKmsKeyId
 - ec2:GetEbsEncryptionByDefault
 - ecs:DescribeClusters
 - eks:DescribeAddonVersions
 - elasticache:DescribeCacheClusters
 - elasticache:DescribeServiceUpdates³⁵³
 - elasticfilesystem:DescribeAccessPoints
 - elasticfilesystem:DescribeFileSystems
-

- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce>ListClusters
- elasticmapreduce>ListSecurityConfigurations
- 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>GetAccountAuthorizationDetails
- iam>GetAccountPasswordPolicy
- iam>GetAccountSummary
- iam>GetCredentialReport
- iam>ListEntitiesForPolicy
- iam>ListGroupPolicies
- iam>ListGroups
- iam>ListOpenIdConnectProviders
- iam>ListPolicies
- 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
- organizations>DescribeOrganization
- organizations>DescribePolicy
- rds>DescribeCertificates
- rds>DescribeDbClusterEndpoints
- rds>DescribeDbClusterParameterGroups
- rds>DescribeDbClusters
- rds>DescribeDBInstances
- rds>DescribeDbSecurityGroups
- redshift>DescribeClusters
- route53>GetQueryLoggingConfig
- s3>GetBucketPublicAccessBlock
- s3>GetBucketVersioning
- s3>GetEncryptionConfiguration
- s3>GetLifecycleConfiguration
- s3>ListAllMyBuckets
- sns>ListTopics
- sqs>ListQueues
- waf-regional>GetLoggingConfiguration
- waf-regional>ListRuleGroups
- waf-regional>ListSubscribedRuleGroups
- waf-regional>ListWebACLs
- waf>ListActivatedRulesInRuleGroup

Note

For more information about the specific API calls that Audit Manager can describe, see [Supported API calls for custom control data sources \(p. 247\)](#).

To view the full permissions details of the service-linked role AWSServiceRoleForAuditManager, see [AWSAuditManagerServiceRolePolicy](#) in the *AWS Managed Policy Reference Guide*.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see [Service-linked role permissions](#) in the *IAM User Guide*.

Creating the AWS Audit Manager service-linked role

onboarding page of the AWS Management Console, or via the API or AWS CLI. For more information, see [Enable AWS Audit Manager \(p. 28\)](#) in this user guide.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account.

Editing the AWS Audit Manager service-linked role

AWS Audit Manager doesn't allow you to edit the AWSServiceRoleForAuditManager service-linked role. After you create a service-linked role, you can't change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see [Editing a service-linked role](#) in the *IAM User Guide*.

To allow an IAM entity to edit the description of the AWSServiceRoleForAuditManager service-linked role

Add the following statement to the permissions policy for the IAM entity that needs to edit the description of a service-linked role.

```
{  
    "Effect": "Allow",  
    "Action": [  
        "iam:UpdateRoleDescription"  
    ],  
    "Resource": "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/  
AWSServiceRoleForAuditManager*",  
    "Condition": {"StringLike": {"iam:AWSServiceName": "auditmanager.amazonaws.com"}}  
}
```

Deleting the AWS Audit Manager service-linked role

If you no longer need to use Audit Manager, we recommend that you delete the AWSServiceRoleForAuditManager service-linked role. That way, you don't have an unused entity that isn't actively monitored or maintained. However, you must clean up the service-linked role before you can delete it.

Cleaning up the service-linked role

Before you can use IAM to delete the Audit Manager service-linked role, you must first confirm that the role has no active sessions and remove any resources used by the role. To do so, ensure that Audit Manager is deregistered in all AWS Regions. After you deregister, Audit Manager no longer uses the service-linked role.

For instructions on how to deregister Audit Manager, see the following resources:

- [Disable AWS Audit Manager \(p. 258\)](#) in this guide
- [DeregisterAccount](#) in the *AWS Audit Manager API Reference*
- [deregister-account](#) in the *AWS CLI Reference for AWS Audit Manager*

For instructions on how to delete Audit Manager resources manually, see [Deletion of Audit Manager data](#) in this guide.

Deleting the service-linked role

You can delete the service-linked role using the IAM console, the AWS Command Line Interface (AWS CLI), or the IAM API.

IAM console

Follow these steps to delete a service-linked role in the IAM console.

To delete a service-linked role (console)

1. Sign in to the AWS Management Console and open the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the navigation pane of the IAM console, choose **Roles**. Then select the check box next to `AWSServiceRoleForAuditManager`, not the name or row itself.
3. Under **Role actions** at the top of the page, choose **Delete**.
4. In the confirmation dialog box, review the last accessed information, which shows when each of the selected roles last accessed an AWS service. This helps you to confirm whether the role is currently active. If you want to proceed, enter `AWSServiceRoleForAuditManager` in the text input field and choose **Delete** to submit the service-linked role for deletion.
5. Watch the IAM console notifications to monitor the progress of the service-linked role deletion. Because the IAM service-linked role deletion is asynchronous, after you submit the role for deletion, the deletion task can succeed or fail. If the task succeeds, then the role is removed from the list and a success message appears at the top of the page.

AWS CLI

You can use IAM commands from the AWS CLI to delete a service-linked role.

To delete a service-linked role (AWS CLI)

1. Enter the following command to list the role in your account:

```
aws iam get-role --role-name AWSServiceRoleForAuditManager
```

2. Because a service-linked role can't be deleted if it's being used or has associated resources, you must submit a deletion request. That request can be denied if these conditions aren't met. You must capture the `deletion-task-id` from the response to check the status of the deletion task.

Enter the following command to submit a service-linked role deletion request:

```
aws iam delete-service-linked-role --role-name AWSServiceRoleForAuditManager
```

3. Use the following command to check the status of the deletion task:

```
aws iam get-service-linked-role-deletion-status --deletion-task-id deletion-task-id
```

The status of the deletion task can be NOT_STARTED, IN_PROGRESS, SUCCEEDED, or FAILED. If the deletion fails, the call returns the reason that it failed so that you can troubleshoot.

IAM API

You can use the IAM API to delete a service-linked role.

To delete a service-linked role (API)

1. Call `GetRole` to list the role in your account. In the request, specify `AWSServiceRoleForAuditManager` as the `RoleName`.

2. Because a service-linked role can't be deleted if it's being used or has associated resources, you must submit a deletion request. That request can be denied if these conditions aren't met. You must capture the `DeletionTaskId` from the response to check the status of the deletion task.

To submit a deletion request for a service-linked role, call [DeleteServiceLinkedRole](#). In the request, specify `AWSServiceRoleForAuditManager` as the `RoleName`.

3. To check the status of the deletion, call [GetServiceLinkedRoleDeletionStatus](#). In the request, specify the `DeletionTaskId`.

The status of the deletion task can be NOT_STARTED, IN_PROGRESS, SUCCEEDED, or FAILED. If the deletion fails, the call returns the reason that it failed so that you can troubleshoot.

Tip

The deletion fails if the Audit Manager service is using the role or has associated resources. This only happens if you're still registered with Audit Manager in one or more AWS Regions. After you deregister, Audit Manager stops using the service-linked role.

To resolve a failed deletion issue, first make sure that you deregistered Audit Manager in all AWS Regions where you used the service. Then, try again to follow the steps in the previous procedure.

Supported Regions for AWS Audit Manager service-linked roles

AWS Audit Manager supports using service-linked roles in all of the AWS Regions where the service is available. For more information, see [AWS service endpoints](#).

Compliance validation for AWS Audit Manager

To learn whether an AWS service is within the scope of specific compliance programs, see [AWS services in Scope by Compliance Program](#) and choose the compliance program that you are interested in. For general information, see [AWS Compliance Programs](#).

You can download third-party audit reports using AWS Artifact. For more information, see [Downloading Reports in AWS Artifact](#).

Your compliance responsibility when using AWS services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- [Security and Compliance Quick Start Guides](#) – These deployment guides discuss architectural considerations and provide steps for deploying baseline environments on AWS that are security and compliance focused.
- [Architecting for HIPAA Security and Compliance on Amazon Web Services](#) – This whitepaper describes how companies can use AWS to create HIPAA-eligible applications.

Note

Not all AWS services are HIPAA eligible. For more information, see the [HIPAA Eligible Services Reference](#).

- [AWS Compliance Resources](#) – This collection of workbooks and guides might apply to your industry and location.
- [Evaluating Resources with Rules](#) in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- [AWS Security Hub](#) – This AWS service provides a comprehensive view of your security state within AWS. Security Hub uses security controls to evaluate your AWS resources and to check your compliance

against security industry standards and best practices. For a list of supported services and controls, see [Security Hub controls reference](#).

- [AWS Audit Manager](#) – This AWS service helps you continuously audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards.

Resilience in AWS Audit Manager

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking.

With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see [AWS Global Infrastructure](#).

Infrastructure security in AWS Audit Manager

As a managed service, AWS Audit Manager is protected by AWS global network security. For information about AWS security services and how AWS protects infrastructure, see [AWS Cloud Security](#). To design your AWS environment using the best practices for infrastructure security, see [Infrastructure Protection](#) in [Security Pillar AWS Well-Architected Framework](#).

You use AWS published API calls to access AWS Audit Manager through the network. Clients must support the following:

- Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3.
- Cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the [AWS Security Token Service](#) (AWS STS) to generate temporary security credentials to sign requests.

You can call these API operations from any network location, but AWS Audit Manager does support resource-based access policies, which can include restrictions based on the source IP address. You can also use Audit Manager policies to control access from specific Amazon Virtual Private Cloud (Amazon VPC) endpoints or specific VPCs. Effectively, this isolates network access to a given Audit Manager resource from only the specific VPC within the AWS network.

AWS Audit Manager and interface VPC endpoints (AWS PrivateLink)

You can establish a private connection between your VPC and AWS Audit Manager by creating an *interface VPC endpoint*. Interface endpoints are powered by [AWS PrivateLink](#), a technology that enables you to privately access Audit Manager APIs without an internet gateway, NAT device, VPN connection, or

AWS Direct Connect connection. Instances in your VPC don't need public IP addresses to communicate with Audit Manager APIs. Traffic between your VPC and AWS Audit Manager does not leave the AWS network.

Each interface endpoint is represented by one or more [Elastic Network Interfaces](#) in your subnets.

For more information, see [Interface VPC endpoints \(AWS PrivateLink\)](#) in the *Amazon VPC User Guide*.

Considerations for AWS Audit Manager VPC endpoints

Before you set up an interface VPC endpoint for AWS Audit Manager, ensure that you review [Interface endpoint properties and limitations](#) in the *Amazon VPC User Guide*.

AWS Audit Manager supports making calls to all of its API actions from your VPC.

Creating an interface VPC endpoint for AWS Audit Manager

You can create a VPC endpoint for the AWS Audit Manager service using either the Amazon VPC console or the AWS Command Line Interface (AWS CLI). For more information, see [Creating an interface endpoint](#) in the *Amazon VPC User Guide*.

Create a VPC endpoint for AWS Audit Manager using the following service name:

- com.amazonaws.*region*.auditmanager

If you enable private DNS for the endpoint, you can make API requests to AWS Audit Manager using its default DNS name for the Region, for example, auditmanager.us-east-1.amazonaws.com.

For more information, see [Accessing a service through an interface endpoint](#) in the *Amazon VPC User Guide*.

Creating a VPC endpoint policy for AWS Audit Manager

You can attach an endpoint policy to your VPC endpoint that controls access to AWS Audit Manager. The policy specifies the following information:

- The principal that can perform actions.
- The actions that can be performed.
- The resources on which actions can be performed.

For more information, see [Controlling access to services with VPC endpoints](#) in the *Amazon VPC User Guide*.

Example: VPC endpoint policy for AWS Audit Manager actions

The following is an example of an endpoint policy for AWS Audit Manager. When attached to an endpoint, this policy grants access to the listed Audit Manager actions for all principals on all resources.

```
{  
    "Statement": [  
        {  
            "Principal": "*",
            "Effect": "Allow",
            "Action": [  
                "auditmanager:GetAssessments",
                "auditmanager:GetServicesInScope",
                "auditmanager>ListNotifications"
            ],
            "Resource": "*"
        }
    ]
}
```

Logging and monitoring in AWS Audit Manager

Monitoring is an important part of maintaining the reliability, availability, and performance of Audit Manager and your other AWS solutions. AWS provides the following monitoring tools to watch Audit Manager, report when something is wrong, and take automatic actions when appropriate:

- *AWS CloudTrail* captures API calls and related events made by or on behalf of your AWS account and delivers the log files to an Amazon S3 bucket that you specify. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred. For more information, see the [AWS CloudTrail User Guide](#).
- *Amazon EventBridge* is a serverless event bus service that makes it easy to connect your applications with data from a variety of sources. EventBridge delivers a stream of real-time data from your own applications, Software-as-a-Service (SaaS) applications, and AWS services and routes that data to targets such as Lambda. This enables you to monitor events that happen in services, and build event-driven architectures. For more information, see the [Amazon EventBridge User Guide](#).

Monitoring AWS Audit Manager with Amazon EventBridge

Amazon EventBridge helps you automate your AWS services and respond automatically to system events such as application availability issues or resource changes.

You can use EventBridge rules to detect and react to Audit Manager events. Based on the rules that you create, EventBridge invokes one or more target actions when an event matches the values that you specify in a rule. Depending on the type of event, you might want to send notifications, capture event information, take corrective action, initiate events, or take other actions.

For example, you can detect whenever the following Audit Manager events occur in your account:

- An audit owner creates, updates, or deletes an assessment
- An audit owner delegates a control set for review
- A delegate completes their review and submits the reviewed control set back to the audit owner
- An audit owner updates the status of an assessment control

The actions that can be automatically triggered include the following:

- Use an AWS Lambda function to pass a notification to a Slack channel.

- Push data about the check to an Amazon Kinesis Data Streams to support comprehensive and real-time status monitoring.
- Send an Amazon Simple Notification Service (Amazon SNS) topic to your email.
- Get notified with an Amazon CloudWatch alarm action.

Note

Audit Manager delivers events on a *durable* basis. This means that Audit Manager will successfully attempt to deliver events to EventBridge at least once. In cases where events can't be delivered because of an EventBridge service disruption, they will be retried again later by Audit Manager for up to 24 hours.

EventBridge example format for Audit Manager

The following JSON code shows an example of an assessment creation event in Audit Manager. For information on any of the fields in this event, see [Event structure reference](#).

```
{  
    "version": "0",  
    "id": "55c5a6f3-6183-3989-49ec-a3c998857644",  
    "detail-type": "Assessment Created",  
    "source": "aws.auditmanager",  
    "account": "111122223333",  
    "time": "2023-07-27T00:38:33Z",  
    "region": "us-west-2",  
    "resources":  
        [  
            "arn:aws:auditmanager:us-west-2:111122223333:assessment/a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6"  
        ],  
    "detail":  
        {  
            "eventID": "4e939b2f-9429-3141-beec-d640d83ef68e",  
            "author": "arn:aws:sts::111122223333:assumed-role/roleName/role-session-name",  
            "assessmentTenantId": "111122223333",  
            "assessmentName": "myAssessment",  
            "eventTime": 1690418289068,  
            "eventName": "CREATE",  
            "eventType": "ASSESSMENT",  
            "assessmentID": "a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6"  
        }  
}
```

Prerequisites for creating an EventBridge rule

Before you create rules for Audit Manager events, we recommend that you do the following:

- Familiarize yourself with events, rules, and targets in EventBridge. For more information, see [What is Amazon EventBridge?](#) in the [Amazon EventBridge User Guide](#).
- Create a target to use in your event rule. For example, you can create an Amazon SNS topic so that whenever a control set review is completed, you'll receive a text message or email. For more information, see [EventBridge targets](#).

Creating an EventBridge rule for Audit Manager

Follow these steps to create an EventBridge rule that triggers on an event emitted by Audit Manager. Events are emitted on a best effort basis.

To create an EventBridge rule for Audit Manager

1. Open the Amazon EventBridge console at <https://console.aws.amazon.com/events/>.
2. In the navigation pane, choose **Rules**.
3. Choose **Create rule**.
4. On the **Define rule detail** page, enter a name and description for the rule.
5. Keep the default values for **Event bus** and **Rule type**, and then choose **Next**.
6. On the **Build event pattern** page, for **Event source**, choose **AWS events or EventBridge partner events**.
7. For **Creation method**, choose **Custom pattern (JSON editor)**.
8. Under **Event pattern**, write an event pattern in JSON and specify the fields that you want to use for matching.

To match an Audit Manager event, you can use the following simple pattern:

```
{  
  "detail-type": ["Event"]  
}
```

Replace **Event** with one of the following supported values:

- a. Enter **Assessment Created** to get notifications when an assessment is created.
- b. Enter **Assessment Updated** to get notifications when an assessment is updated.
- c. Enter **Assessment Deleted** to get notifications when an assessment is deleted.
- d. Enter **Assessment ControlSet Delegation Created** to get notifications when a control set is delegated for review.
- e. Enter **Assessment ControlSet Reviewed** to get notifications when an assessment control set is reviewed.
- f. Enter **Assessment Control Reviewed** to get notifications when an assessment control is reviewed.

Tip

Add more fields to your event pattern as needed. For more information about available fields, see [Amazon EventBridge event patterns](#).

9. Choose **Next**.
10. On the **Select target(s)** page, choose the target that you created for this rule, and then configure any additional options that are required for that type. For example, if you choose Amazon SNS, make sure that your SNS topic is configured correctly so that you'll be notified by email or SMS.

Tip

The fields displayed vary depending on the service selected. For more information about available targets, see [Targets available in the EventBridge console](#).

11. For many target types, EventBridge needs permissions to send events to the target. In these cases, EventBridge can create the IAM role that's needed for your rule to run.
 - a. To create an IAM role automatically, choose **Create a new role for this specific resource**.
 - b. To use an IAM role that you created earlier, choose **Use existing role**.
12. (Optional) Choose **Add another target** to add another target for this rule.
13. Choose **Next**.
14. (Optional) On the **Configure tags** page, add any tags and then choose **Next**.
15. On the **Review and create** page, review your rule setup and ensure that it meets your event monitoring requirements.

16. Choose **Create rule**. Your rule will now monitor for Audit Manager events and then send them to the target that you specified.

Logging AWS Audit Manager API calls with CloudTrail

Audit Manager is integrated with CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Audit Manager. CloudTrail captures all API calls for Audit Manager as events. The calls captured include calls from the Audit Manager console and code calls to the Audit Manager API operations.

If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Audit Manager. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**.

Using the information collected by CloudTrail, you can determine the request that was made to Audit Manager, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the [AWS CloudTrail User Guide](#).

Audit Manager information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Audit Manager, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**.

You can view, search, and download recent events in your AWS account. For more information, see [Viewing Events with CloudTrail Event History](#).

For an ongoing record of events in your AWS account, including events for Audit Manager, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify.

Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- [Overview for Creating a Trail](#)
- [CloudTrail Supported Services and Integrations](#)
- [Configuring Amazon SNS Notifications for CloudTrail](#)
- [Receiving CloudTrail Log Files from Multiple Regions](#) and [Receiving CloudTrail Log Files from Multiple Accounts](#)

All Audit Manager actions are logged by CloudTrail and are documented in the [AWS Audit Manager API Reference](#). For example, calls to the `CreateCustomControl`, `DeleteControl` and `UpdateAssessmentTemplate` API operations generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the [CloudTrail userIdentity Element](#).

Understanding Audit Manager Log File Entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the [CreateAssessment](#) action.

```
{  
    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"
```

Configuration and vulnerability analysis in AWS Audit Manager

Configuration and IT controls are a shared responsibility between AWS and you, our customer. For more information, see the AWS [shared responsibility model](#).

Tagging AWS Audit Manager resources

A *tag* is a metadata label that you assign or that AWS assigns to an AWS resource. Each tag consists of a *key* and a *value*. For tags that you assign, you define the key and value. For example, you might define the key as stage and the value for one resource as test.

Tags help you do the following:

- Easily locate your Audit Manager resources. You can use tags as search criteria when browsing the framework library and the control library.
- Associate your resource with a compliance type. You can tag multiple resources with a compliance-specific tag to associate those resources with a specific framework.
- Identify and organize your AWS resources. Many AWS services support tagging, so you can assign the same tag to resources from different services to indicate that the resources are related.
- Track your AWS costs. You activate these tags on the AWS Billing and Cost Management dashboard. AWS uses the tags to categorize your costs and deliver a monthly cost allocation report to you. For more information, see [Use cost allocation tags](#) in the *AWS Billing and Cost Management User Guide*.

The following sections provide more information about tags for AWS Audit Manager.

Supported resources in Audit Manager

The following Audit Manager resources support tagging:

- Assessments
- Controls
- Frameworks

Tag restrictions

The following basic restrictions apply to tags on Audit Manager resources:

- Maximum number of tags that you can assign to a resource — 50
- Maximum key length — 128 Unicode characters
- Maximum value length — 256 Unicode characters
- Valid characters for key and value — a-z, A-Z, 0-9, space, and the following characters: _ . : / = + - and @
- Keys and values are case sensitive
- Don't use aws : as a prefix for keys; it's reserved for AWS use

Managing tags

You can set tags as properties when you create an assessment, framework, or control. You can add, edit, and delete tags through the Audit Manager console, the AWS Command Line Interface (AWS CLI), and the Audit Manager API. For more information, see the following links.

- For assessments:
 - [Creating an assessment \(p. 50\)](#) and [Editing an assessment \(p. 54\)](#) in the *Assessments* section of this guide
 - [Tags tab \(p. 60\)](#) in the *Review an assessment* section of this guide
 - [CreateAssessment](#) and [UpdateAssessment](#) in the *AWS Audit Manager API Reference*
 - [TagResource](#) and [UntagResource](#) in the *AWS Audit Manager API Reference*
- For frameworks:
 - [Creating a custom framework \(p. 110\)](#) and [Editing a custom framework \(p. 114\)](#) in the *Framework library* section of this guide
 - [Tags tab](#) in the *View framework details* section of this guide
 - [CreateAssessmentFramework](#) and [UpdateAssessmentFramework](#) in the *AWS Audit Manager API Reference*
 - [TagResource](#) and [UntagResource](#) in the *AWS Audit Manager API Reference*
- For controls:
 - [Creating a custom control \(p. 203\)](#) and [Editing a custom control \(p. 208\)](#) in the *Control library* section of this guide
 - [Tags tab](#) in the *View control details* section of this guide
 - [CreateControl](#) and [UpdateControl](#) in the *AWS Audit Manager API Reference*
 - [TagResource](#) and [UntagResource](#) in the *AWS Audit Manager API Reference*

Creating AWS Audit Manager resources with AWS CloudFormation

AWS Audit Manager is integrated with AWS CloudFormation, a service that helps you to model and set up your AWS resources so that you can spend less time creating and managing your resources and infrastructure. You create a template that describes all the AWS resources that you want (such as assessments), and AWS CloudFormation provisions and configures those resources for you.

When you use AWS CloudFormation, you can reuse your template to set up your Audit Manager resources consistently and repeatedly. Describe your resources once, and then provision the same resources over and over in multiple AWS accounts and Regions.

Audit Manager and AWS CloudFormation templates

To provision and configure resources for Audit Manager and related services, you must understand [AWS CloudFormation templates](#). Templates are formatted text files in JSON or YAML. These templates describe the resources that you want to provision in your AWS CloudFormation stacks. If you're unfamiliar with JSON or YAML, you can use AWS CloudFormation Designer to help you get started with AWS CloudFormation templates. For more information, see [What is AWS CloudFormation Designer?](#) in the [AWS CloudFormation User Guide](#).

Audit Manager supports creating assessments in AWS CloudFormation. For more information, including examples of JSON and YAML templates for assessments, see the [AWS Audit Manager resource type reference](#) in the [AWS CloudFormation User Guide](#).

Learn more about AWS CloudFormation

To learn more about AWS CloudFormation, see the following resources:

- [AWS CloudFormation](#)
- [AWS CloudFormation User Guide](#)
- [AWS CloudFormation API Reference](#)
- [AWS CloudFormation Command Line Interface User Guide](#)

Document history for AWS Audit Manager User Guide

The following table describes the important changes in each release of the AWS Audit Manager User Guide from December 8, 2020, onward.

Change	Description	Date
Support for AWS Security Hub consolidated control findings (p. 370)	Audit Manager now supports consolidated controls in AWS Security Hub. For more information, see AWS Security Hub controls supported by AWS Audit Manager .	November 16, 2023
Integration with MetricStream (p. 370)	You can now ingest evidence from Audit Manager into MetricStream. For more information, see Integrations with third-party GRC products .	November 14, 2023
New supported framework: AWS generative AI best practices (p. 370)	A new prebuilt framework is now available in AWS Audit Manager. For more information, see AWS generative AI best practices framework v1 .	November 8, 2023
Updated AWS managed policy (p. 370)	AWS Audit Manager has updated the AWSAuditManagerServiceRolePolicy . For more information, see AWS managed policies for AWS Audit Manager .	November 6, 2023
Integration with Amazon EventBridge (p. 370)	You can now monitor events that happen in AWS Audit Manager and use these events as part of your event-driven architecture. For more information, see Monitoring AWS Audit Manager with Amazon EventBridge .	August 18, 2023
Support for risk assessments and new manual evidence options (p. 370)	You can now use the custom control creation workflow to support risk assessments. A control can now represent a risk assessment question, and you can provide an answer by uploading a file or entering text as manual evidence. For more information, see Create a custom control and Add manual evidence .	June 12, 2023

<u>Support for CSV exports (p. 370)</u>	You can now export your evidence finder search results in CSV format. For more information, see <u>Export your search results</u> .	June 9, 2023
<u>New supported framework: Australian Cyber Security Centre (ACSC) Information Security Manual (p. 370)</u>	A new prebuilt framework is now available in AWS Audit Manager. For more information, see <u>Australian Cyber Security Centre (ACSC) Information Security Manual</u> .	March 24, 2023
<u>Improved assessment reports (p. 370)</u>	We made improvements to the format and contents of Audit Manager assessment reports. For more information about how to navigate and understand assessment reports, see <u>Assessment reports</u> .	March 23, 2023
<u>Support for paginated API calls (p. 370)</u>	AWS Audit Manager now supports paginated API calls as a data source for evidence collection. For more information, see <u>Paginated API calls</u> .	March 8, 2023
<u>New supported framework: HIPAA Final Omnibus Security Rule 2013 (p. 370)</u>	A new prebuilt framework is now available in AWS Audit Manager. For more information, see <u>HIPAA Final Omnibus Security Rule 2013</u> . For differentiation purposes, the previously existing HIPAA framework (formerly named <i>HIPAA</i> in the framework library) is now named <u>HIPAA Security Rule 2003</u> .	March 8, 2023
<u>Support for additional AWS API calls (p. 370)</u>	You can now use an additional nine AWS API calls as a data source for your custom controls in Audit Manager. For more information, see <u>Supported API calls for custom control data sources</u> .	March 3, 2023
<u>Updated guide to align with the IAM best practices (p. 370)</u>	Updated guide to align with the IAM best practices. For more information, see <u>Security best practices in IAM</u> .	January 6, 2023
<u>New data retention setting (p. 370)</u>	You can now specify if you want to delete all of your data when you disable Audit Manager. For more information, see <u>Disable AWS Audit Manager</u> and <u>Deletion of Audit Manager data</u> .	January 6, 2023

<u>Support for evidence finder (p. 370)</u>	You can now use evidence finder to perform search queries on your evidence data. For more information, see Evidence finder .	November 18, 2022
<u>New supported framework: Australian Cyber Security Centre (ACSC) Essential Eight (p. 370)</u>	A new prebuilt framework is now available in AWS Audit Manager. For more information, see Australian Cyber Security Centre (ACSC) Essential Eight .	August 24, 2022
<u>Updated AWS managed policy (p. 370)</u>	AWS Audit Manager has updated the AWSAuditManagerServiceRolePolicy . For more information, see AWS managed policies for AWS Audit Manager .	July 7, 2022
<u>Updated AWS managed policy (p. 370)</u>	AWS Audit Manager has updated the AWSAuditManagerServiceRolePolicy . For more information, see AWS managed policies for AWS Audit Manager .	May 20, 2022
<u>New supported framework: Canadian Centre for Cyber Security Medium Cloud Control Profile (p. 370)</u>	A new prebuilt framework is now available in AWS Audit Manager. For more information, see Canadian Centre for Cyber Security Medium Cloud Control Profile .	May 6, 2022
<u>Updated AWS managed policy (p. 370)</u>	AWS Audit Manager has updated the AWSAuditManagerAdministratorAccess policy. For more information, see AWS managed policies for AWS Audit Manager .	April 29, 2022
<u>Support for additional AWS Config managed rules (p. 370)</u>	You can now use an additional 91 AWS Config managed rules as a data source for your custom controls in Audit Manager. For more information, see Using AWS Config managed rules with AWS Audit Manager .	April 27, 2022
<u>Support for AWS Config custom rules (p. 370)</u>	You can now use AWS Config custom rules as a data source for your custom controls in Audit Manager. For more information, see Using AWS Config custom rules with AWS Audit Manager .	April 27, 2022
<u>New supported framework: ISO/IEC 27001:2013 Annex A (p. 370)</u>	A new prebuilt framework is now available in AWS Audit Manager. For more information, see ISO/IEC 27001:2013 Annex A .	April 7, 2022

<u>Updated AWS managed policy (p. 370)</u>	AWS Audit Manager has updated the AWSAuditManagerServiceRolePolicy . For more information, see AWS managed policies for AWS Audit Manager .	March 16, 2022
<u>New supported frameworks: CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4 (p. 370)</u>	Two new prebuilt frameworks are now available in AWS Audit Manager: <i>CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4</i> , <i>Level 1</i> , and <i>CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4, Level 1 and 2</i> . For more information, see CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.4.0 .	March 2, 2022
<u>New supported framework: CIS Controls v8 IG1 (p. 370)</u>	A new prebuilt framework is now available in AWS Audit Manager. For more information, see CIS Controls v8 IG1 .	March 2, 2022
<u>AWS Audit Manager dashboard (p. 370)</u>	You can now use the Audit Manager dashboard to monitor your active assessments and quickly identify non-compliant evidence. For more information, see Using the Audit Manager dashboard .	November 18, 2021
<u>Custom framework sharing (p. 370)</u>	You can now share your custom Audit Manager frameworks with another AWS account, or replicate them into another AWS Region under your own account. For more information, see Sharing a custom framework .	October 22, 2021
<u>New examples of AWS Audit Manager controls (p. 370)</u>	You can now review examples of controls and learn how Audit Manager helps bring your AWS environment in line with their requirements. For more information, see Examples of AWS Audit Manager controls .	September 21, 2021
<u>New supported framework: Gramm-Leach-Bliley Act (GLBA) (p. 370)</u>	A new prebuilt framework is now available in AWS Audit Manager. For more information, see Gramm-Leach-Bliley Act (GLBA) .	September 2, 2021

<u>New troubleshooting chapter (p. 370)</u>	A new troubleshooting chapter is now available. For more information, see <u>Troubleshooting in AWS Audit Manager</u> .	August 23, 2021
<u>New delegation chapter and tutorial (p. 370)</u>	We expanded our delegation documentation into a new chapter. For more information, see <u>Delegations in AWS Audit Manager</u> . We also added a new tutorial aimed at delegates who are reviewing a control set for the first time in AWS Audit Manager. For more information, see <u>Tutorial for Delegates: Reviewing a control set</u> .	June 25, 2021
<u>New supported framework: NIST SP 800-171 Rev. 2 (p. 370)</u>	A new prebuilt framework is now available in AWS Audit Manager. For more information, see <u>NIST SP 800-171 Rev. 2</u> .	June 17, 2021
<u>Improved assessment reports (p. 370)</u>	We made improvements to the format and contents of AWS Audit Manager assessment reports. For more information about how to navigate and understand the new assessment reports, see <u>Assessment reports</u> .	June 8, 2021
<u>New AWS managed policies page (p. 370)</u>	AWS Audit Manager has started tracking changes for its managed policies. For more information, see <u>AWS managed policies for AWS Audit Manager</u> .	May 6, 2021
<u>New supported framework: NIST Cybersecurity Framework version 1.1 (p. 370)</u>	A new prebuilt framework is now available in AWS Audit Manager. For more information, see <u>NIST Cybersecurity Framework version 1.1</u> .	May 5, 2021
<u>New supported framework: AWS Well-Architected (p. 370)</u>	A new prebuilt framework is now available in AWS Audit Manager. For more information, see <u>AWS Well-Architected</u> .	May 5, 2021
<u>New supported framework: AWS Foundational Security Best Practices (p. 370)</u>	A new prebuilt framework is now available in AWS Audit Manager. For more information, see <u>AWS Foundational Security Best Practices</u> .	May 5, 2021
<u>New supported framework: GxP EU Annex 11 (p. 370)</u>	A new prebuilt framework is now available in AWS Audit Manager. For more information, see <u>GxP EU Annex 11</u> .	April 28, 2021

<u>New supported framework: NIST 800-53 (Rev. 5) Low-Moderate-High (p. 370)</u>	A new prebuilt framework is now available in AWS Audit Manager. For more information, see <u>NIST 800-53 (Rev. 5) Low-Moderate-High</u> .	March 25, 2021
<u>New supported frameworks: CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3 (p. 370)</u>	Two new prebuilt frameworks are now available in AWS Audit Manager: <i>CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0, Level 1</i> , and <i>CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0, Level 1 and 2</i> . For more information, see <u>CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0</u> .	March 22, 2021
<u>Initial release (p. 370)</u>	Initial release of the AWS Audit Manager User Guide and API Reference.	December 8, 2020

AWS Glossary

For the latest AWS terminology, see the [AWS glossary](#) in the *AWS Glossary Reference*.