
AWS Audit Manager

User Guide



AWS Audit Manager: User Guide

Copyright © 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 AWS Audit Manager?	2
More AWS Audit Manager resources	2
Concepts and terminology	2
Evidence collection	6
Evidence collection frequency	7
Examples of controls	7
Automated controls (Security Hub)	8
Automated controls (AWS Config)	9
Automated controls (API calls)	10
Automated controls (CloudTrail)	11
Manual controls	13
Controls with mixed data sources	14
Related services	16
Setting up	18
Step 1: Sign up for AWS	18
Step 2: Attach the required IAM policy to an IAM identity	18
Step 3: Enable AWS Organizations (optional)	19
Create or join an organization	20
Enable all features	20
Designate a delegated administrator	20
Configure your organization's AWS Security Hub settings	21
Step 4: Enable AWS Audit Manager	21
Service-linked role	24
What do I do next?	24
Get started	24
Update your settings	24
Getting started	25
Audit Manager tutorials	25
Tutorial for Audit Owners: Creating an assessment	25
Step 1: Specify assessment details	26
Step 2: Specify accounts in scope	26
Step 3: Specify services in scope	27
Step 4: Specify audit owners	27
Step 5: Review and create	27
Where do I go from here?	28
Tutorial for Delegates: Reviewing a control set	28
Step 1: Access your notifications	29
Step 2: Review control set and evidence	29
Step 3: Upload manual evidence	30
Step 4: Add a comment	31
Step 5: Update control status	31
Step 6: Submit the reviewed control set back to the audit owner	31
Where do I go from here?	32
Assessments	33
Creating an assessment	33
Step 1: Specify assessment details	34
Step 2: Specify accounts in scope	34
Step 3: Specify services in scope	35
Step 4: Specify audit owners	35
Step 5: Review and create	36
What can I do next?	36

Accessing an assessment	36
Editing an assessment	37
Step 1: Edit assessment details	37
Step 2: Edit accounts in scope	37
Step 3: Edit services in scope	38
Step 4: Edit audit owners	38
Step 5: Review and save	38
Reviewing an assessment	39
Assessment details	39
Controls tab	40
Assessment report selection tab	40
AWS accounts tab	41
AWS services tab	41
Audit owners tab	41
Tags tab	42
Changelog tab	42
Reviewing controls	42
Control detail	43
Control status	43
Evidence folders tab	43
Data source tab	44
Comments tab	44
Changelog tab	45
Reviewing evidence	45
Reviewing evidence folders	46
Reviewing individual evidence	47
Uploading manual evidence	49
Generating an assessment report	50
Adding evidence	50
Generating the report	50
Changing an assessment status	51
Deleting an assessment	52
Delegations	53
For audit owners	53
Delegating a control set	53
Accessing delegations	55
Deleting delegations	55
For delegates	56
Viewing notifications	56
Reviewing controls and evidence	57
Adding comments	58
Marking a control as reviewed	58
Submitting a control set to the audit owner	58
Assessment reports	60
How to navigate a report	60
Report sections	60
Cover page	61
Overview	61
Table of contents	62
Control set page	62
Control page	62
Evidence summary page	63
Evidence detail page	64
Report integrity check	64
Troubleshooting	65
My assessment report failed to generate	65
Failed report generation	65

Unable to unzip report	65
I get an <i>access denied</i> error when I try to generate a report	66
My assessment report generation is stuck in <i>In progress</i> status, and I'm not sure how this impacts my billing	66
Assessment report destinations	66
Configuration tips	67
Issues to consider	67
Framework library	69
Accessing a framework	69
Viewing framework details	70
Framework details	70
Control sets	71
Tags tab	71
Creating a custom framework	71
Create new	71
Customize existing	73
Editing a custom framework	74
Step 1: Specify framework details	75
Step 2: Edit controls	75
Step 3: Review and update	76
Deleting a custom framework	76
Supported frameworks	76
AWS Audit Manager Sample Framework	77
AWS Control Tower Guardrails	77
AWS License Manager	78
AWS Foundational Security Best Practices	79
AWS Operational Best Practices (OBP)	79
AWS Well-Architected	80
CIS AWS Foundations Benchmark v.1.2	81
CIS AWS Foundations Benchmark v.1.3	82
CIS Controls	83
FedRAMP Moderate Baseline by Allgress	84
GDPR	85
Gramm-Leach-Bliley Act	100
GxP 21 CFR part 11	101
GxP EU Annex 11	101
HIPAA	102
HITRUST	103
NIST 800-53 (Rev. 5)	104
NIST CSF v1.1	105
NIST SP 800-171 (Rev. 2)	106
PCI DSS	107
SOC 2	108
Control library	109
Accessing a control	109
Viewing control details	110
Control summary	110
Control details tab	110
Tags tab	111
Creating a custom control	111
Create new	111
Customize existing	114
Editing a custom control	117
Step 1: Edit control details	117
Step 2: Edit data sources	117
Step 3: Edit action plan	119
Step 4: Review and update	119

Deleting a custom control	119
Changing evidence collection frequency	119
Configuration snapshots from API calls	120
Compliance checks from AWS Config	121
Compliance checks from Security Hub	121
User activity logs from AWS CloudTrail	121
Control data sources	122
AWS Config	122
AWS Security Hub	126
AWS API calls	127
AWS CloudTrail	128
Settings	129
Permissions	129
Data encryption	129
Default audit owners (optional)	130
Assessment report destination (optional)	130
Notifications (optional)	131
Delegated administrator (optional)	131
AWS Config (optional)	132
Security Hub (optional)	133
Disable AWS Audit Manager	133
Notifications	134
Prerequisites	134
Configuring notifications in AWS Audit Manager	134
Troubleshooting	135
I specified an Amazon SNS topic in Audit Manager, but I'm not receiving any notifications	135
Troubleshooting	136
Evidence collection	136
I created an assessment but I can't see any evidence yet	136
My assessment isn't collecting any evidence from AWS Security Hub	137
My assessment isn't collecting evidence from another AWS service	138
My evidence is generated at different intervals, and I don't understand how often it's being collected	138
Permissions and access	139
I followed the Audit Manager setup procedure, but I don't have enough IAM privileges	139
I specified someone as an audit owner, but they still don't have full access to the assessment. Why is this?	140
I can't perform an action in Audit Manager	140
I'm an administrator and want to allow others to access Audit Manager	140
I want to allow people outside of my AWS account to access my Audit Manager resources	140
Controls and control sets	141
I can't see any controls or control sets in my assessment	141
I can't upload manual evidence to a control	141
Assessment reports	141
My assessment report failed to generate	142
I followed the checklist above, and my assessment report still failed to generate	142
I'm unable to unzip the assessment report	142
I get an <i>access denied</i> error when I try to generate a report	143
My assessment report generation is stuck in <i>In progress</i> status, and I'm not sure how this impacts my billing	143
Delegated administrators	143
I can't set up Audit Manager with my delegated administrator account	144
When I create an assessment, I can't see the accounts from my organization under <i>Accounts in scope</i>	144
I get an <i>access denied</i> error when I try to generate an assessment report using my delegated administrator account	144
Notifications	145

I specified an Amazon SNS topic in Audit Manager, but I'm not receiving any notifications	145
Quotas	146
Security	147
Data protection	147
Encryption at rest	148
Encryption in transit	148
Key management	149
Identity and access management	149
Audience	150
Authenticating with identities	150
Managing access using policies	152
How AWS Audit Manager works with IAM	153
Identity-based policy examples	159
AWS managed policies	168
Troubleshooting	176
Using service-linked roles	178
Compliance validation	180
Resilience	180
Infrastructure security	181
VPC endpoints (AWS PrivateLink)	181
Considerations for AWS Audit Manager VPC endpoints	181
Creating an interface VPC endpoint for AWS Audit Manager	181
Creating a VPC endpoint policy for AWS Audit Manager	182
Logging and monitoring	182
CloudTrail logs	183
Configuration and vulnerability	185
Tagging resources	186
Supported resources	186
Tag restrictions	186
Managing tags in AWS Audit Manager	186
AWS CloudFormation resources	188
Audit Manager and AWS CloudFormation templates	188
Learn more about AWS CloudFormation	188
Using the AWS SDKs	189
AWS SDK for .NET	189
AWS SDK for C++	189
AWS SDK for Go	189
AWS SDK for Java 2.x	190
AWS SDK for JavaScript	190
AWS SDK for PHP V3	190
AWS SDK for Python (Boto)	190
AWS SDK for Ruby V3	190
Document history	191
AWS glossary	193

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.

AWS 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, AWS 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 AWS Audit Manager

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

- **Get started quickly** — Select 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.
- **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, HITRUST, SOC2, GxP, and AWS operational best practices.
- **Customize frameworks** — Create your own frameworks with standard or custom controls based on your specific requirements for internal audits.
- **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 AWS Audit Manager

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

Are you a first-time user of AWS 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 AWS 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 AWS Audit Manager resources

Explore the following resources to learn more about AWS 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.

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 the framework of your choice 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 \(p. 33\)](#).

Assessment report

An assessment report is a finalized document that's generated from an AWS 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 \(p. 60\)](#). To learn how to generate an assessment report, see [Generating an assessment report \(p. 50\)](#).

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 an IAM 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](#).

Changelog

For each control in an assessment, AWS 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 \(p. 45\)](#).

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, HIPAA, and HITRUST.

Control

A control is a prescriptive description that describes how to conform to a given rule. It provides an assurance that the resources that are used by your organization operate as intended, that data is reliable, and that your organization is in compliance with applicable laws and regulations. A compliance standard or regulation contains multiple controls, which are grouped into control sets.

There are two types of control in AWS Audit Manager:

- **Standard controls** — Predefined controls that are based on AWS best practices for several compliance standards and regulations. You can use these controls to assist you with audit preparation for common compliance standards and regulations.
- **Custom controls** — Customized controls that you define as an AWS Audit Manager user. You can use these controls to help you meet your specific compliance requirements.

For more information, see [Examples of AWS Audit Manager controls](#). For instructions on how to create and manage controls, see [Control library \(p. 109\)](#).

Control data source

A control data source defines the resource where AWS Audit Manager collects evidence from to support the requirements of a control. Examples in AWS include the following data sources:

- AWS CloudTrail log
- AWS Config rule
- AWS Security Hub check
- Amazon EC2 instance
- Amazon S3 bucket
- AWS Identity and Access Management (IAM) user or role
- Network component such as an Amazon Virtual Private Cloud (VPC), security group, or network access control list (ACL) table

A single control can have multiple data sources.

Delegate

A delegate is an AWS Audit Manager user with limited permissions. Delegates typically have specialized business or technical expertise. For example, these expertises 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 \(p. 53\)](#).

Evidence

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

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

- **Automated evidence** — This is the evidence that AWS 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, with varied frequencies (for example, you can use AWS Security Hub to configure periodic checks every 12 hours or continually if invoked by change events). Examples of compliance checks include a security check in AWS Security Hub for a PCI DSS control and an AWS Config rule evaluation from AWS Config for HIPAA.
 - **User activity** — User activity that changes a resource configuration is captured from AWS CloudTrail logs as that activity occurs. Examples of user activities include a route table update, an Amazon RDS instance backup setting change, and an Amazon S3 bucket encryption policy change.
 - **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 Amazon S3 bucket encryption policy.
- **Manual evidence** — This is the evidence that you can upload to AWS Audit Manager manually as an additional support document.

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 \(p. 6\)](#). For instructions on how to review evidence in an assessment, see [Reviewing the evidence in an assessment \(p. 45\)](#).

Framework

An AWS 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 AWS 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 AWS 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 \(p. 69\)](#).

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.

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, AWS 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

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 data sources 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, AWS 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

AWS 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 AWS 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 AWS 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 checks supported by AWS Audit Manager](#) (p. 126).
 - 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. 122).
- **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. 128).
- **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. 109). For more information about how Audit Manager uses API calls to create evidence, see [API calls supported by AWS Audit Manager](#) (p. 127).

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 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](#). 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 \(p. 8\)](#)
- [Automated controls that use AWS Config as a data source \(p. 9\)](#)
- [Automated controls that use AWS API calls as a data source \(p. 10\)](#)
- [Automated controls that use AWS CloudTrail as a data source \(p. 11\)](#)
- [Manual controls \(p. 13\)](#)
- [Controls with mixed data sources \(automated and manual\) \(p. 14\)](#)

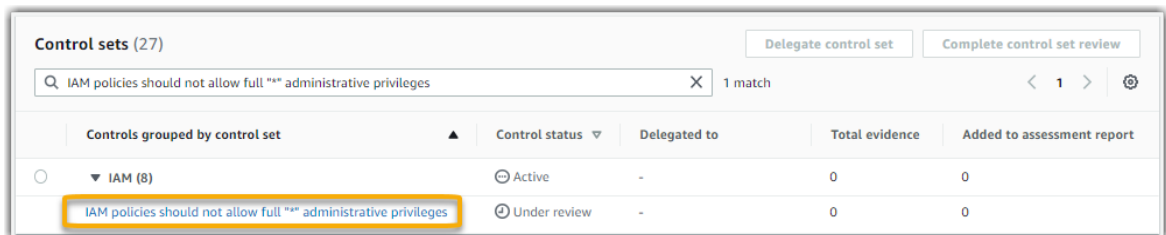
Automated controls that use AWS Security Hub as a data source

This example shows a control that uses AWS Security Hub as its data source. 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** – 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 > ⚙	
Controls grouped by control set ▲		Control status ▼	Delegated to	Total evidence	Added to assessment report
▼ IAM (8)		⊕ Active	-	0	0
IAM policies should not allow full "*" administrative privileges		⊕ 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 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. 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. This evidence contains the original data that's captured from your IAM policies, the Security Hub ruling, 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 `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.

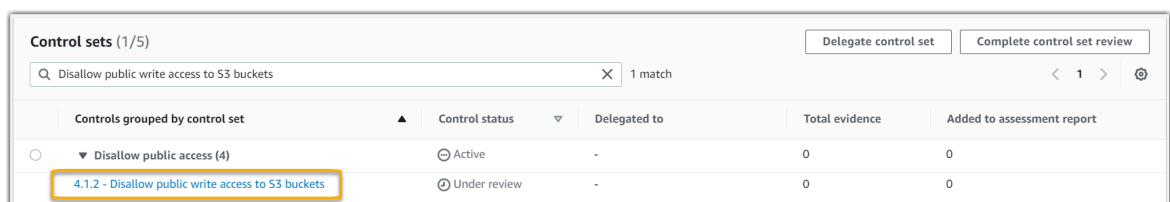
Automated controls that use AWS Config as a data source

This example shows a control that uses AWS Config as its data source. 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** – 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)		Delegate control set		Complete control set review	
Q Disallow public write access to S3 buckets X 1 match		< 1 > @			
Controls grouped by control set		Control status	Delegated to	Total evidence	Added to assessment report
<input type="radio"/>	▼ Disallow public access (4)	⊖ Active	-	0	0
<input type="radio"/>	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. 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. This evidence contains the original data that's captured from your S3 bucket resources, the AWS Config ruling, 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 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.

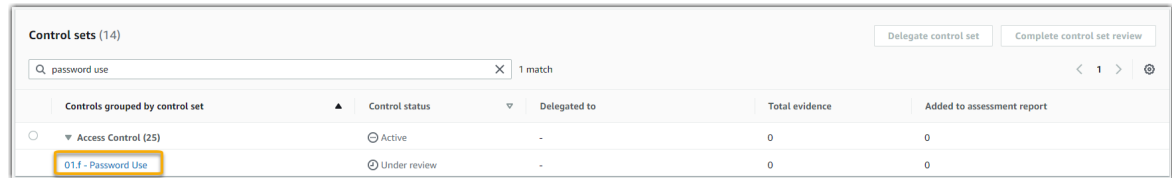
Automated controls that use AWS API calls as a data source

This example shows a control that uses AWS API calls as its data source. This is a standard control taken from the [HITRUST v9.4 - Level 1 framework](#). Audit Manager uses this control to generate evidence that can help to bring your AWS environment in line with HITRUST requirements.

Example control details

- **Control name** – 01.f – Password Use
- **Control set** – This control belongs to the Access Control control set. This is a grouping of controls that relate to identity and access management.
- **Data source** – AWS API calls
- **Evidence type** – Configuration data

In the following example, this control is within an Audit Manager assessment that was created from the HITRUST v9.4 - Level 1 framework.



Controls grouped by control set	Control status	Delegated to	Total evidence	Added to assessment report
Access Control (25)	Active	-	0	0
01.f - Password Use	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 help you ensure that you have sufficient access control policies in place. The 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 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 an API call is the data source. 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 control in your assessment that's named `01.f - 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 IAM 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 like, 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 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

This example shows a control that uses AWS CloudTrail as its data source. 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 called 164.308 Administrative Safeguards.
- **Data source** – AWS CloudTrail
- **Evidence type** – User activity

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

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, 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 usernames 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 IAM users are the resource, and CloudTrail logs are the data source. 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. This evidence contains the original data that's captured from your IAM 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 IAM 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** – 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:

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, 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 (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 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 a 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 sources (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** – 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
<input type="text" value="Citizenship Requirements for Classified Systems"/> 1 match		< 1 >	🔍
Controls grouped by control set	Control status	Delegated to	Total evidence
<input type="radio"/> Maintenance Personnel (6)	⌚ Active	-	0
<input type="radio"/> MA-5(3) - Citizenship Requirements for Classified Systems	⌚ Under review	-	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 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 need to 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 a series of API calls are 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. 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 [Uploading 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 IAM users. If you're not sure how to identify which users are maintenance personnel, or what the citizenship of those users is, 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 IAM 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.

Related AWS services

AWS Audit Manager integrates with multiple AWS services to automatically collect evidence and generate assessment reports.

AWS Security Hub

AWS Security Hub monitors your environment using automated security checks based on AWS best practices and industry standards. AWS Audit Manager imports Security Hub findings for supported compliance standards and regulations. These include the CIS Foundations Benchmark and PCI DSS. Audit Manager automatically performs additional analysis and adds annotations to the collected Security Hub findings to generate evidence for the AWS services that are monitored by Security Hub. For more information about AWS Security Hub, see [What is AWS Security Hub?](#) in the *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, AWS CLI, and other AWS services. AWS Audit Manager directly collects log data from AWS CloudTrail directly and performs additional analysis. It annotates the data to generate evidence automatically for over 175 AWS services that feed logs into AWS CloudTrail. For more information about AWS 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. AWS Audit Manager collects log data from AWS Config and performs additional analysis. It annotates that data to generate evidence automatically for the AWS services that AWS Config monitors. 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. AWS Audit Manager imports license usage limits and the usage data over time from License Manager. For more information on License Manager, see [What is AWS License Manager?](#) in the *License Manager User Guide*.

AWS Control Tower

AWS Control Tower enforces preventative and detective guardrails for cloud infrastructure. AWS Audit Manager imports guardrail logs, and maps them to user events gathered from CloudTrail, and AWS

Config as evidence of compliance or non-compliance to the guardrails. It then uses this data to generate assessment reports for your audit. 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](#).

Setting up AWS Audit Manager

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

Topics

- [Step 1: Sign up for AWS](#) (p. 18)
- [Step 2: Attach the required IAM policy to an IAM identity](#) (p. 18)
- [Step 3: Enable AWS Organizations](#) (optional) (p. 19)
- [Step 4: Enable AWS Audit Manager](#) (p. 21)
- [What do I do next?](#) (p. 24)

Step 1: Sign up for AWS

If you don't already have an AWS account, you must create one. For more information, see [How to create and activate a new AWS account](#).

Step 2: Attach the required IAM policy to an IAM identity

The AWS Identity and Access Management (IAM) identity (user, role, or group) that you use to access AWS Audit Manager must have the required permissions. Admin roles have these permissions by default.

To grant the permissions required to use Audit Manager, attach the following policy to an IAM identity. For more information about how to attach a policy to an IAM identity, see [Adding and removing IAM identity permissions](#) in the *IAM User Guide*.

Note

What we provide here is a basic policy that allows you to register AWS Audit Manager. This guide also provides some [examples of other permission policies](#) that you can use in Audit Manager. The [Creating an assessment tutorial for audit owners](#) in this guide assumes that you are a user with administrator or management permissions. 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](#).

```
{
  "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": {
            "StringEquals": {
                "events:source": "aws.securityhub",
                "events:detail-type": "Security Hub Findings - Imported"
            }
        }
    },
    {
        "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"
            }
        }
    }
]
}
```

For more information about IAM and how it works with AWS Audit Manager, see [Identity and access management for AWS Audit Manager \(p. 149\)](#) in this guide.

Step 3: Enable AWS Organizations (optional)

AWS 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.

If you don't need multi-account support from Audit Manager, you don't need to enable AWS Organizations and you can skip the following tasks. Instead, you can create and run assessments for a single AWS account.

Tasks to enable AWS Organizations

- [Create or join an organization \(p. 20\)](#)

- [Enable all features in your organization](#) (p. 20)
- [Designate a delegated administrator for AWS Audit Manager](#) (p. 20)
- [Configure your organization's AWS Security Hub settings](#) (p. 21)

Create or join an organization

If your AWS account is not yet part of an organization, you can create or join an organization as described in [Creating and managing an organization](#) in the *AWS Organizations User Guide*.

Enable all features in your organization

In order to collect evidence from the accounts in your organization, AWS Audit Manager requires that you [enable all features in your organization](#).

After your account is a member of an organization and you have enabled all features in your organization, you can designate a delegated administrator account for AWS Audit Manager.

Designate a delegated administrator for AWS Audit Manager

If you already use AWS Organizations and want to enable multi-account support from AWS Audit Manager, you can designate a delegated administrator account for Audit Manager.

We recommend that you enable AWS Audit Manager using an AWS Organizations management account, and then designate 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 designate a delegated administrator using an AWS Organizations management account, your management account can no longer create additional assessments in AWS Audit Manager. Additionally, evidence collection stops for any existing assessments 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 designate a delegated administrator

- To add a delegated administrator when you set up Audit Manager for the first time, follow the instructions in [Step 4: Enable AWS Audit Manager](#) (p. 21).
- To add or change a delegated administrator at a later date, see [AWS Audit Manager settings, Delegated administrator](#).

Issues to consider

- 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, you should 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 review and change your encryption settings, see [Data encryption](#) (p. 129).

Configure your organization's AWS Security Hub settings

In order for AWS Audit Manager to collect AWS Security Hub evidence from your member accounts, you must perform the following steps in Security Hub.

Note

You must make sure that the delegated administrator account that you designate in Security Hub is the same one that you designate in Audit Manager.

To configure 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*.
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. 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*.

Step 4: Enable AWS Audit Manager

After you attach the required policy to an IAM identity, you can use that identity to enable AWS Audit Manager.

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

Enable AWS Audit Manager (console)

To enable AWS 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 the IAM identity to sign in.
3. Choose **Set up AWS Audit Manager**.
4. Under **Permissions**, no action is required by default. This is because Audit Manager uses a service-linked role to connect to data sources on your behalf. If needed, 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 a AWS KMS key for securely storing your data. If you want to use your own customer managed keys to encrypt data in Audit Manager, choose **Customize encryption settings (advanced)**. You can then choose an existing KMS key or create a new one.

For more information about how to set up customer managed keys, see [Creating keys](#) in the *AWS Key Management Service User Guide*.

6. (Optional) Under **Delegated administrator - optional**, you can designate a delegated administrator account if you want Audit Manager to run assessments for multiple accounts.

Note

- When you designate a delegated administrator account using an AWS Organizations management account, you must make sure that the delegated administrator account has access on the KMS key provided during step 5.
 - If you want to enable AWS Audit Manager in more than one AWS Region, you must assign a delegated administrator account separately in each Region.
 - We recommend that you enable Audit Manager using an AWS Organizations management account, and then add a delegated administrator in your [AWS Audit Manager settings](#). 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 AWS Organizations management account.
7. (Optional) Under **AWS Config - optional**, we recommend that you enable AWS Config for an optimal experience. This allows Audit Manager to generate evidence using AWS Config rules. For more information about how to enable AWS Config, see [Setting up AWS Config](#) in the *AWS Config User Guide*. You can choose to enable AWS Config at a later time from your [AWS Audit Manager settings](#).
 8. (Optional) Under **AWS Security Hub - optional**, we recommend that you enable Security Hub for an optimal experience. This allows Audit Manager to generate evidence using Security Hub checks. For more information about how to enable Security Hub, see [Setting up AWS Security Hub](#) in the *AWS Security Hub User Guide*. You can choose to enable Security Hub at a later time from your [AWS Audit Manager settings](#).
 9. Choose **Complete setup** to finish the setup process.

Enable AWS Audit Manager (API)

To enable AWS Audit Manager using the Audit Manager API

1. Use the [RegisterAccount](#) operation.
2. Use the following setup parameters:
 - a. `kmsKey` (optional) - You can use this parameter to encrypt your data within Audit Manager using your KMS key.
 - b. `delegatedAdminAccount` (optional) - You can use this parameter to designate your AWS organization's `delegatedAdminAccount` for Audit Manager.

Note

- When you designate a delegated administrator account using an AWS Organizations management account, you must make sure that the delegated administrator account has access on the KMS key provided during step 2a.
- If you want to enable Audit Manager in more than one AWS Region, you must assign a delegated administrator account separately in each Region.
- We recommend that you enable Audit Manager using an AWS Organizations management account, and then set up 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 AWS Organizations management account.

Input example:

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

Output example:

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

Enable AWS Audit Manager (AWS CLI)

To enable AWS Audit Manager using the AWS CLI

1. At the command line, run the [register-account](#) command.
2. Use the following setup parameters:
 - a. `--kms-key` (optional) - You can use this parameter to encrypt your data within Audit Manager using your KMS key.
 - b. `--delegated-admin-account` (optional) - You can use this parameter to designate your AWS organization's delegated administrator account for Audit Manager.

Note

- When you designate a delegated administrator account using an AWS Organizations management account, you must make sure that the delegated administrator account has access on the KMS key provided during step 2a.
- If you want to enable AWS Audit Manager in more than one AWS Region, you must assign a delegated administrator account separately in each Region.
- We recommend that you enable AWS Audit Manager using an AWS Organizations management account, and then set up 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 AWS Organizations management account.

Input example:

```
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 -> (string)
```

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](#)

Service-linked role assigned to AWS Audit Manager

When you enable AWS Audit Manager, it is assigned a service-linked role named `AWSServiceRoleForAuditManager`. This service-linked role includes the policy that enables Audit Manager to do the following on your behalf:

- Collect and assess data from the following data sources to generate AWS Audit Manager evidence:
 - Management events from AWS CloudTrail
 - Compliance checks from AWS Config Rules
 - Compliance checks from AWS Security Hub
- Describe APIs specific to the following services:
 - AWS CloudTrail
 - Amazon CloudWatch
 - Amazon Cognito user pools
 - AWS Config
 - Amazon EC2
 - Amazon EFS
 - Amazon EventBridge
 - Amazon GuardDuty
 - AWS Identity and Access Management (IAM)
 - AWS KMS
 - AWS License Manager
 - AWS Organizations
 - Amazon Route 53
 - Amazon S3
 - AWS Security Hub
 - AWS WAF

You can view the details of the service-linked role `AWSServiceRoleForAuditManager` in the console. Choose **Getting started**, choose **Permissions**, and then choose **View IAM service-linked role permissions**. For more information, see [Using service-linked roles for AWS Audit Manager \(p. 178\)](#).

For more information about service-linked roles, see [Using service-linked roles](#) in the *IAM User Guide*.

What do I do next?

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

Get started with AWS 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 AWS Audit Manager settings

You can modify your settings at any time. For more information, see [AWS Audit Manager settings \(p. 129\)](#).

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. 154).

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 \(p. 18\)](#). 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 \(p. 186\)](#).
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.

Note

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 [Step 3: Enable AWS Organizations \(optional\)](#) (p. 19) on the *Setting up* page of this guide.

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 select a standard framework, the list of 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 data sources and services for you. This selection is made according to the requirements of the standard framework.

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. 69) 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**.

Note

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.

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 \(p. 7\)](#) 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 \(p. 39\)](#) – Introduces you to the assessment page where you can explore the different components of your assessment.
- [Assessments in AWS Audit Manager \(p. 33\)](#) – 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 \(p. 69\)](#) – Introduces the framework library and explains how to [create a custom framework](#) for your own specific compliance needs.
- [Control library \(p. 109\)](#) – 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 \(p. 18\)](#).
- 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 IAM 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. 31).

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 \(p. 39\)](#) - 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.

Assessments in AWS Audit Manager

An Audit Manager assessment is based on a framework, which is a grouping of controls. Using the framework of your choice 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 AWS 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 [AWS Audit Manager concepts and terminology](#).

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 \(p. 33\)](#)
- [Accessing your assessments in AWS Audit Manager \(p. 36\)](#)
- [Editing an assessment \(p. 37\)](#)
- [Reviewing an assessment \(p. 39\)](#)
- [Reviewing the controls in an assessment \(p. 42\)](#)
- [Reviewing the evidence in an assessment \(p. 45\)](#)
- [Uploading manual evidence in AWS Audit Manager \(p. 49\)](#)
- [Generating an assessment report \(p. 50\)](#)
- [Changing the status of an assessment to inactive \(p. 51\)](#)
- [Deleting an assessment \(p. 52\)](#)

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 the framework of your choice. Follow these steps to create an assessment and start the ongoing collection of evidence.

Tasks

- [Step 1: Specify assessment details \(p. 34\)](#)
- [Step 2: Specify AWS accounts in scope \(p. 34\)](#)
- [Step 3: Specify AWS services in scope \(p. 35\)](#)

- [Step 4: Specify audit owners](#) (p. 35)
- [Step 5: Review and create](#) (p. 36)
- [What can I do next?](#) (p. 36)

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 in.
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.
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 AWS Audit Manager, see [Tagging AWS Audit Manager resources](#) (p. 186).
8. Choose **Next**.

Tip

- To learn more about a framework before selecting one, choose the framework name. This opens the framework summary page. On this page, you can review the contents of that framework, such as all of its controls and data sources.
- The default assessment report destination is based on your AWS Audit Manager settings. For more information, see [AWS Audit Manager settings, Assessment report destination](#). If you'd prefer, you can create and use multiple S3 buckets to help you organize your assessment reports.

Step 2: Specify AWS accounts in scope

Specify the accounts to include in the scope of your assessment.

You can specify multiple AWS accounts to be in the scope of an assessment. AWS 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 AWS Audit Manager, see [Step 3: Enable AWS Organizations \(optional\)](#) (p. 19).

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 AWS 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, AWS 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 haven't subscribed to 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

If you selected a standard framework in [step 1](#), the list of AWS services in scope is selected by default and can't be edited. This is because when you create an assessment from a standard framework, 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 proceed, review the list and choose **Next**.

Tip

If you've selected a standard framework and you want to be able to edit the services in scope, we recommend that you [customize the framework](#) and then use the custom framework to create your assessment.

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 IAM 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.
 - If you're an administrator and you need to create a new IAM identity for an audit owner, see [I'm an administrator and want to allow others to access AWS Audit Manager \(p. 177\)](#).
 - If you want to create a new IAM identity for an audit owner and you don't have the permissions to do so, contact your administrator for assistance. Your administrator is the person who provided you with your user name and password.
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. AWS 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 \(p. 7\)](#) 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 \(p. 39\)](#)
- [Editing an assessment \(p. 37\)](#)
- [Reviewing the controls in an assessment \(p. 42\)](#)
- [Reviewing the evidence in an assessment \(p. 45\)](#)
- [Uploading manual evidence to an assessment](#)
- [Delegations in AWS Audit Manager \(p. 53\)](#)
- [Generating an assessment report \(p. 50\)](#)
- [Changing the status of an assessment](#)
- [Deleting an assessment \(p. 52\)](#)

Accessing your assessments in AWS Audit Manager

You can find a list of all your active assessments and your inactive past assessments on the **Assessments** page in AWS Audit Manager. From the assessments page, you can also [edit an assessment](#), [delete an assessment](#), or [create an assessment](#).

To access your assessments

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 associated controls and other details for that assessment.

Editing an assessment

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

Tasks

- [Step 1: Edit assessment details \(p. 37\)](#)
- [Step 2: Edit AWS accounts in scope \(p. 37\)](#)
- [Step 3: Edit AWS services in scope \(p. 38\)](#)
- [Step 4: Edit audit owners \(p. 38\)](#)
- [Step 5: Review and save \(p. 38\)](#)

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 \(p. 42\)](#). 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 to include in the scope of your assessment.

You can specify multiple AWS accounts to be in the scope of an assessment. AWS 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](#).

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 haven't subscribed to it in your environment, then Audit Manager won'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

If you created the assessment 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 you created the assessment 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**.

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 AWS 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.

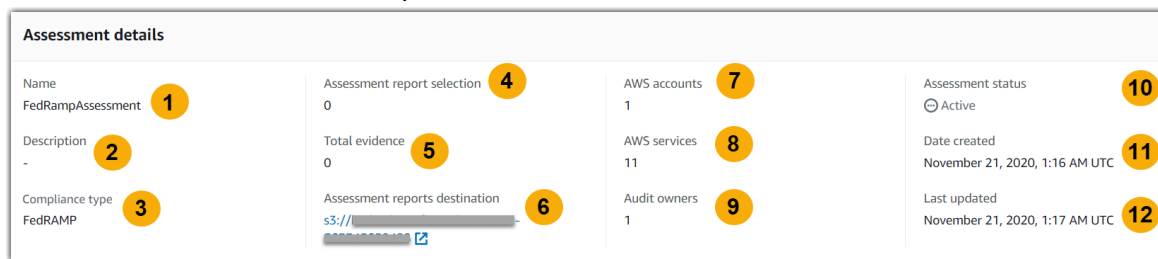
When you open an assessment, you will see a summary page that contains several sections. The sections of this page and their contents are described as follows.

Sections of the assessment page

- [Assessment details](#) (p. 39)
- [Controls tab](#) (p. 40)
- [Assessment report selection tab](#) (p. 40)
- [AWS accounts tab](#) (p. 41)
- [AWS services tab](#) (p. 41)
- [Audit owners tab](#) (p. 41)
- [Tags tab](#) (p. 42)
- [Changelog tab](#) (p. 42)

Assessment details

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



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 AWS 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.

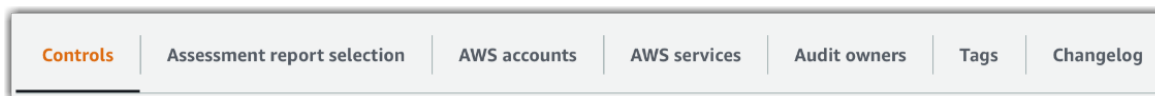
10 **Assessment status** – The status of the assessment.

- **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 \(p. 51\)](#).

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 hasn't yet been 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.
- **Added to assessment report** – The number of evidence items that are associated with the control that are included in the assessment report.

Assessment report selection tab



The **Assessment report selection** tab displays the list of evidence to be included in the assessment report, grouped by evidence folders. These evidence folders are both 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 detail** dashboard at the top of the page.

Under the **Assessment report selection** table, a list of evidence folders is displayed with the following data columns:

- **Evidence folder** – The name of the evidence folder. The folder name is based on the date on which 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 associated with this evidence folder.

For information about adding evidence to an assessment report, see [Generating an assessment report](#) (p. 50).

AWS accounts tab

Controls	Assessment report selection	AWS accounts	AWS services	Audit owners	Tags	Changelog
----------	-----------------------------	---------------------	--------------	--------------	------	-----------

The **AWS accounts** 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 detail** dashboard at the top of the page.

Under the **AWS accounts** table, a list of accounts is displayed with the following data columns:

- **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

Controls	Assessment report selection	AWS accounts	AWS services	Audit owners	Tags	Changelog
----------	-----------------------------	--------------	---------------------	--------------	------	-----------

The **AWS services** tab displays the list of AWS services that are in the scope of the assessment. The total number of services is summarized under the **Assessment detail** dashboard at the top of the page.

Under the **AWS services** table, a list of services is displayed with the following data columns:

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

Audit owners tab

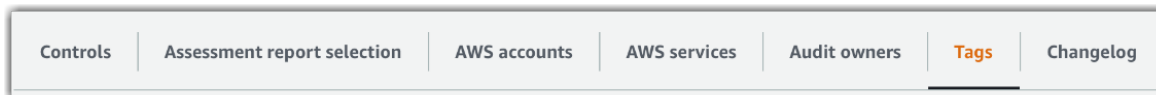
Controls	Assessment report selection	AWS accounts	AWS services	Audit owners	Tags	Changelog
----------	-----------------------------	--------------	--------------	---------------------	------	-----------

The **Audit owners** tab displays the audit owners for the assessment. The total number of audit owners is also summarized under the **Assessment detail** dashboard at the top of the page.

Under the **Audit owners** table, a list of accounts is displayed with the following data columns:

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

Tags tab



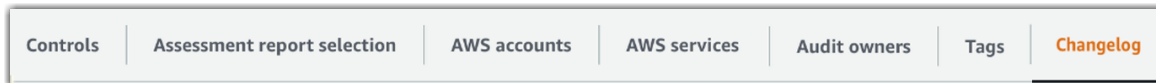
The **Tags** tab displays the list of tags inherited from the framework are used to create this assessment. The total number of tags is summarized under **Assessment detail** at the top of the page.

Under the **Tags** table, a list of tags is displayed with the following data columns:

- **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 \(p. 186\)](#).

Changelog tab



The **Changelog** tab displays a list of user activity related to the assessment.

Under the **Changelog** table, a list of accounts is displayed with the following data columns:

- **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 from which the assessment was created.

Reviewing the controls in an assessment

Controls in AWS 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. 43)
- [Update control status](#) (p. 43)
- [Evidence folders tab](#) (p. 43)
- [Data source tab](#) (p. 44)
- [Comments tab](#) (p. 44)
- [Changelog tab](#) (p. 45)

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 controls in the assessment.

The following statuses are available for a control:

- **Under review** – Indicates that this control hasn't yet been 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 has been reviewed. Evidence is still being collected, and you can upload manual evidence.
- **Inactive** – Indicates that automated evidence collection has 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 is organized into folders on a daily basis. From here, you can also select a folder and choose **Upload manual evidence** to add more evidence manually.

Under the **Evidence folders** table, a list of folders is displayed with the following data columns:

- **Evidence folder** – The name of the evidence folder. The name is based on the date when the evidence was collected.
- **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. You can find more information about the relevant evidence and the nature of the issue by opening the evidence folder.

Not applicable indicates that you either don't have AWS Security Hub or AWS Config enabled, or the evidence comes from a different data source.

- **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, choose a folder to open an [Reviewing evidence folders \(p. 46\)](#). From the evidence folder summary page, you can choose an evidence item to open an [Reviewing individual evidence \(p. 47\)](#).

From the **Evidence folders** tab, you can also choose to add or remove evidence to an assessment report. For more information, see [Generating an assessment report \(p. 50\)](#).

Data source tab



The **Data source** tab displays the data sources for the control.

Under the **Data source** table, a list of data sources is displayed with the following data columns.

- **Name** – The name of the data source from which AWS Audit Manager collects evidence.
- **Data source** – The name of the AWS service that contains this data.
- **Attribute** – The associated attribute value for retrieving the data from the data source. For example, this can be the parameter attribute used when making a describe API call to an AWS service.
- **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 \(p. 7\)](#).

Comments tab

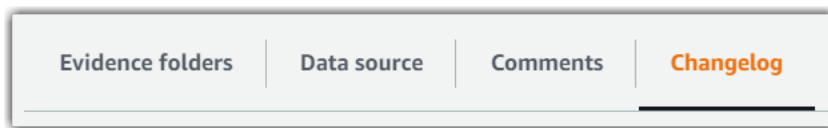


In the **Comments** tab, you can add a comment regarding the control and its evidence. It also displays a list of previous comments.

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 AWS 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.
- **User** – The IAM 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.

AWS 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 AWS Audit Manager automatically collects evidence from a range of data sources. For more information, see [How AWS Audit Manager collects evidence \(p. 6\)](#). 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.

- 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 \(p. 46\)](#)
- [Reviewing individual evidence \(p. 47\)](#)

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 \(p. 46\)](#)
- [Evidence table \(p. 47\)](#)

Evidence folder summary

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

Summary			
Evidence folder details		Evidence by type	
Date 1	Added to assessment report 3	User Activity 6	Compliance check 9
8/10/2020, 00:00 UTC - 23:59 UTC	0	1	2
Control name 2	Total evidence 4	Configuration data 7	Compliance check status 10
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating ...	5	1	1 issue found
Resources 5	8	Manual 8	
		1	

It includes the following information:

- Date** – The time and date when the evidence folder was created.
- Control name** – The name of the control that's associated with the evidence folder.
- Added to assessment report** – The number of evidence items that were manually selected for inclusion in the assessment report.
- Total evidence** – The total number of evidence items in the evidence folder.
- Resources** – The total number of AWS resources that were assessed when generating the evidence in this folder.
- User activity** – The number of evidence items that fall under the *user activity* category. This evidence is collected from AWS CloudTrail logs.
- 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.
- Manual** – The number of evidence items that fall under the *manual* category. This evidence is uploaded manually.
- 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.
- 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 [AWS Audit Manager concepts and terminology \(p. 2\)](#).

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. 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 is collected from AWS Security Hub, a **Pass** or **Fail** result is reported directly from AWS Security Hub.
 - For evidence that is 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.
4. **Data source** – The AWS service from which the evidence is collected.
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 \(p. 48\)](#)
- [Attributes \(p. 48\)](#)
- [Resources included \(p. 49\)](#)

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
Evidence folder name 2 2020-08-10	Event name 5 UpdateAccountPasswordPolicy	Compliance check 8 Not applicable	Account name (# 12)
Control name 3 Ensure IAM password policy requires minimum password length of 20 or greater	Data source 6 AWS CloudTrail	Resources included 9 2	IAM ID 12
		Attributes 10 4	Added to assessment report 13 No

It includes the following information:

1. **Date and time** – The date and time the evidence was collected.
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 AWS service 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 IAM user or role ID, if applicable.
- 13 **Added to assessment report** – Indicates whether 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.

Uploading manual evidence in AWS Audit Manager

Although AWS Audit Manager automatically collects evidence for many of the controls in your selected framework, some controls require that you upload manual evidence to demonstrate compliance for that control. For example, if a control in your framework is a procedural control that covers your team's organization, you can upload your company's organizational chart manually as evidence to support the control.

You can upload manual evidence from any Amazon Simple Storage Service (Amazon S3) bucket by specifying the S3 URI of the evidence. Your manual evidence must be uploaded to your S3 bucket before you can upload it to your assessment. For more information, 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. 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. Choose the **Evidence folders** tab, and then choose **Upload manual evidence**. Or, you can choose an evidence folder name in the **Evidence folders** tab to review the evidence folder summary page, 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 more information, see [Update control status \(p. 43\)](#).

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

Generating an assessment report

An assessment report summarizes your assessment and provides links to an organized set of folders containing related evidence. For more information, see [Assessment reports \(p. 60\)](#).

You can choose which evidence you want to include in your assessment report before generating the assessment report.

Tasks

- [Adding evidence to an assessment report \(p. 50\)](#)
- [Generating the assessment report \(p. 50\)](#)

Adding evidence to an assessment report

Before you generate an assessment report, you should review the evidence for each control in your assessment and specify whether you want to include it in the assessment report. By default, newly collected evidence is excluded from the assessment report.

To review and include evidence in 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. Scroll down to the **Controls** table, and choose the name of the control to open the control details page.
4. Scroll down to the **Evidence folders** table, select the evidence folder that you want to add to the assessment report, and then choose **Add to assessment report**. In the pop-up window that appears, choose **Add to assessment report** to confirm the addition.
 - If you want to remove an evidence folder that was previously added to an evidence report, select the folder and choose **Remove from assessment report**.
5. To add a single evidence item to an assessment report, choose the name of the evidence folder to open the evidence folder summary page. Select the evidence, and then choose **Add to assessment report**. In the pop-up window that appears, choose **Add to assessment report** to confirm the addition.
 - If you want to remove a single evidence item that was previously added to an assessment report, choose the name of the evidence folder to open the evidence folder summary page. Select the evidence, and then choose **Remove from assessment report**.
6. After you review the evidence and added it to an assessment report, a green success banner appears. Choose **View assessment report selection** to go back to the assessment page, where you can now generate an assessment report.

Generating the assessment report

After you select the evidence to include in your assessment report, you can generate the final assessment report to share with your auditors.

When you generate an assessment report, it is placed into the S3 bucket that you designated as your assessment report destination.

Tip

We recommend that you verify the following configurations before you generate your report:

1. The AWS Region of your assessment report destination (and your customer managed key, if you provided one) must match the AWS Region of your assessment.
2. 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 you configured in your AWS 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 more information about how to configure the assessment report destination and the KMS key used for data encryption, see [AWS Audit Manager settings \(p. 129\)](#). For a list of Audit Manager Regions, see [AWS Regions and Endpoints](#) in the *Amazon Web Services General Reference*.

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 for which you want to generate an assessment report.
4. Choose the **Assessment report selection** tab, and then choose **Generate assessment report**.
5. In the pop-up window, provide a name and description for the assessment report, and review the **Assessment report details** section. This includes the assessment name, the evidence in the assessment report, and the assessment report destination (the S3 bucket that you specified when creating the assessment).
6. Choose **Generate assessment report**.

You can now go to the S3 bucket that you designated as your destination folder and download the assessment report. The generated assessment report has a file checksum to ensure the integrity of the assessment report. You can validate this with the [ValidateAssessmentReportIntegrity](#) API operation offered by AWS Audit Manager.

Changing the status of an assessment to inactive

When you no longer need AWS 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 be certain 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.

To change an assessment status to inactive

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.

Deleting an assessment

You can delete an assessment that you no longer want in AWS Audit Manager.

To delete an assessment

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.

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 \(p. 53\)](#)
- [Delegation tasks for delegates \(p. 56\)](#)

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 \(p. 53\)](#)
- [Accessing your active and completed delegations \(p. 55\)](#)
- [Deleting your active and completed delegations \(p. 55\)](#)

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.
 - If you're an administrator and you need to create a new user or role, see [I'm an administrator and want to allow others to access AWS Audit Manager \(p. 177\)](#).
 - If you want to create a new user or role and you don't have the permissions to do so, contact your administrator for assistance. Your administrator is the person that provided you with your user name and password.
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.
 - If you're an administrator and you need to create a new user or role, see [I'm an administrator and want to allow others to access AWS Audit Manager \(p. 177\)](#).
 - If you want to create a new user or role and you don't have the permissions to do so, contact your administrator for assistance. Your administrator is the person that provided you with your user name and password.
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 \(p. 56\)](#).

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 IAM 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 \(p. 154\)](#).

Delegation tasks

- [Viewing your notifications for incoming delegation requests \(p. 56\)](#)
- [Reviewing the delegated control set and its related evidence \(p. 57\)](#)
- [Adding a comment to a control \(p. 58\)](#)
- [Marking a control as reviewed \(p. 58\)](#)
- [Submitting the reviewed control set back to the audit owner \(p. 58\)](#)

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 IAM 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 AWS Audit Manager *assessment report* summarizes the selected evidence that was collected for an assessment. It also contains links to evidence PDF files that contain the supporting evidence. The specific contents, organization, and naming conventions of assessment reports depend on the parameters that you choose when generating the report.

When you generate an assessment report from an active AWS Audit Manager assessment, you can select which evidence you want to include in the report. The assessment report is then placed in your specified Amazon S3 bucket. For more information, see [Generating an assessment report \(p. 50\)](#).

Assessment reports are designed to help you select and compile the evidence that is relevant for your audit, but they do not assess the compliance of the evidence itself. Instead, AWS Audit Manager simply provides all of the selected evidence as output.

How to navigate an assessment report

Assessment reports begin with a high-level overview. This includes a summary of the assessment report itself, along with a summary of the assessment that the report was created from.

After you've read the overview, you can use the table of contents (TOC) to navigate the rest of the report. Choose any hyperlinked control set or control in the TOC to jump directly to that item and read more details. From here, you can either return to the TOC to choose a different control or control set, or continue reading to see the detailed breakdown of a control's evidence.

When you're ready to review evidence for a control, you can do so by choosing the hyperlinked evidence name. For automated evidence, choosing the hyperlinked evidence name opens a new PDF file with a summary and further details about that evidence. These evidence PDF files are included as part of the assessment report package that you download from AWS Audit Manager. For manual evidence, the hyperlink takes you to the S3 bucket that contains the manual evidence.

Tip

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

Report sections

The following sections provide information about each section of the assessment report. Choose a topic to learn more about that section and reference its data definitions.

Note

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

- [Cover page \(p. 61\)](#)
- [Overview \(p. 61\)](#)
- [Table of contents \(p. 62\)](#)
- [Control set page \(p. 62\)](#)
- [Control page \(p. 62\)](#)
- [Evidence summary page \(p. 63\)](#)
- [Evidence detail page \(p. 64\)](#)

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 assessment report.

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

Assessment report name

Report generated on *MM/DD/YYYY* at *HH:MM:SS AM/PM UCT* by *AccountID* from the following assessment: *Assessment name*

Overview

The overview contains two parts: a summary of the report itself, and a summary of the assessment that the report was generated from.

Assessment report summary

The following information is included in the assessment report summary.

- **Assessment report name** – The name of the report.
- **Assessment 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).
- **Control sets** – The number of control sets in the report.
- **Controls** – The total number of controls in the report.
- **AWS Region in scope** – The AWS Region where the report was created.
- **AWS accounts in scope** – The list of AWS account IDs that are included in the scope of the report.
- **AWS services in scope** – The list of AWS services that are included in the scope of the report.
- **Compliance check status** – The total number of compliance check issues that are found in the report.
- **Assessment report selection** – The number of evidence items that are selected for inclusion in the report.

Assessment summary

The following information is included in the assessment summary.

- **Assessment name** – The name of the assessment that the report was generated from.
- **Audit owner** – The AWS Identity and Access Management (IAM) user or role for the audit owner.
- **Date created** – The date when the assessment was created. The time is represented in UTC.
- **Last updated** – The date when the assessment was last updated. The time is represented in UTC.
- **Assessment status** – The status of the assessment at the time when the assessment report was generated.
- **AWS Region in scope** – The AWS Region that's in the scope of the assessment.
- **AWS accounts in scope** – The list of AWS account IDs that are in the scope of the assessment.
- **AWS services in scope** – The 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.

- **Framework description** – The optional description of the framework that the assessment was created from.
- **Framework type** – Specifies whether the framework is a standard or custom framework.
- **Compliance type** – The name of the compliance standard or regulation that the framework supports.

Table of contents

The table of contents 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 always nested 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 set page

You can use the control set summary to familiarize yourself with the control set before choosing a particular control to review.

Control set summary

The following information is included in the control set summary.

- **Control set name** – The name of the control set.
- **Control set status** – The review status of the control set at the time when the report was generated.
- **Total controls** – The total number of controls in the control set.
- **Compliance check status** – The number of compliance check issues found for this control set, out of all of the evidence that was selected for inclusion in the assessment report for the given control set.
- **Assessment report selection** – The number of evidence items from this control set that were included in the report.
- **Controls** – The list of controls that are part of the control set. Choose the hyperlinked control to go directly to the page in the report that contains more information about that control.

Control page

The control page contains two parts: a summary of the control itself and a summary of the related evidence for that control that was included in the report.

Control summary

The following information is included in the control summary.

- **Control name** – The name of the control.
- **Control set** – The name of the control set that the control belongs to.
- **Control description** – The description of the control.
- **Testing information** – The recommended testing procedures for this control.
- **Action plan** – The recommended actions to perform if the control is not fulfilled.
- **First evidence collection date** – The date and time when the first piece of evidence was collected for this control. The time is represented in UTC.
- **Last evidence collection date** – The date and time when the last piece of evidence was collected for this control. The time is represented in UTC.

- **Compliance check status** – The number of compliance check issues that were found for this control's evidence.
- **Assessment report selection** – The number of evidence items related to this control that were included in the assessment report.

Assessment report selection

In the assessment report selection table, a list of evidence folders is displayed with the following data columns.

- **Evidence name** – Displays the evidence grouped by folders. These folders are then organized and named by the date on which the evidence was collected. Following each folder name in bold is a list of hyperlinked evidence names.
 - Automated evidence names begin with date of the automated evidence collection, followed by a unique identifier and the *_auto* suffix (for example, [\[HH-MM-SSAM/PMUTC\]_\[abcdefghij\]_auto](#)). For automated evidence, the hyperlinked name opens a new PDF file with a summary and further details about that evidence.
 - Manual evidence names begin with the date of the manual upload, followed by a unique identifier, the first 10 characters of the filename, and the file extension (for example, [\[HH-MM-SSAM/PMUTC\]_\[abcdefghij\]_ManualEvid.csv](#)). For manual evidence, the hyperlinked name takes you to the S3 bucket that contains the manual evidence object.
- **Compliance check status** – Next to each evidence folder name is the total number of compliance check issues for that folder. For each evidence row under that folder, the **Compliance check status** column displays the result of the corresponding compliance check.
 - For automated evidence that's collected from AWS Security Hub, a **Passed**, **Failed**, **Warning**, or **Not applicable** result is reported directly from Security Hub. For more information about these statuses, see [Determining the overall status of a control from its findings](#) in the *Security Hub User Guide*.
 - For automated evidence that's collected from AWS Config, a **Compliant**, **Non compliant**, or **Not applicable** result is reported directly from AWS Config. For more information about these statuses, see [Compliance](#) in the *AWS Config API Reference*.
 - For automated evidence that's collected from AWS CloudTrail and API calls, and for all manual evidence, **Not applicable** appears.

Evidence summary page

The following information is included in the evidence summary.

- **Evidence name** – The name of the evidence. The name is based on the date when the evidence was created or uploaded on.
- **Evidence folder** – The name of the folder where the evidence is located. The name is based on the date when the evidence was created on, recorded in the [\[YYYY-MM-DD\]](#) format.
- **Evidence description** – The description of the evidence. It includes the related AWS account and the source where the evidence was collected from.
- **Assessment report name** – The name of the report.
- **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.
- **Framework description** – The optional description for the framework.
- **Framework type** – Specifies whether the framework is a standard or custom framework.
- **Compliance type** – The compliance standard or regulation that the framework supports.
- **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 IAM 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 is not 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 \(p. 64\)](#) of the evidence PDF.
- **Event name** – The name of the evidence event.
- **Event time** – The time when the evidence event occurred.
- **Data source** – The name of the AWS service that the evidence was collected from.
- **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 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, a **Passed**, **Failed**, **Warning**, or **Not applicable** result is reported directly from Security Hub. For more information about these statuses, see [Determining the overall status of a control from its findings](#) in the *Security Hub User Guide*.
 - For automated evidence that's collected from AWS Config, a **Compliant**, **Non compliant**, or **Not applicable** result is reported directly from AWS Config. For more information about these statuses, see [Compliance](#) in the *AWS Config API Reference*.
 - For automated evidence that's collected from AWS CloudTrail and API calls, and for all manual evidence, **Not applicable** appears.

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 control, the contents of the evidence detail page vary. For example, evidence details from an API call consist of a list of the API parameters in a tabular format, and the corresponding responses for each element.

Tip

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

Assessment report integrity check

When you generate assessment reports for your audit, AWS Audit Manager produces a report file checksum so that you can validate that the report remains unaltered. You can download the report to share evidence with your auditors.

To validate the integrity of a report, use the [ValidateAssessmentReportIntegrity](#) API provided by AWS Audit Manager.

Troubleshooting assessment reports

Use the information here to help you troubleshoot and fix issues that you might encounter when working with assessment reports in Audit Manager.

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 S3 bucket match the AWS Region of your assessment?** The S3 bucket that you use as your assessment report destination must be in the same AWS Region as your assessment. For instructions on how to change the S3 bucket, see [AWS Audit Manager settings, Assessment report destination](#).
 - b. **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 [AWS Audit Manager settings, Data encryption](#).
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 configure the assessment report destination and the KMS key that's used for data encryption, see [AWS Audit Manager settings](#).

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 can support up to approximately 22,000 evidence items in a single assessment report. If you try to generate a report that contains more evidence than this, the operation might fail.

If you encounter this issue, we recommend that you generate multiple assessment reports as a workaround. This will allow you to export evidence from your assessment into more manageable-sized batches.

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.

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 AWS 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 key 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.

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](#).

Assessment report destinations

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 specify your preferred

assessment report destination when you first create your assessment. For instructions on how to update your preferences, see [Settings](#), [Assessment report destination](#) in this guide.

Configuration tips

To ensure the successful publication of your assessment report, we recommend that you verify the following configurations for your assessment report destination.

AWS Region

The AWS Region of your assessment report destination (and your customer managed key, if you provided one) must match the AWS Region of your assessment. For instructions on how to configure the assessment report destination and the KMS key used for data encryption, see [AWS Audit Manager settings](#). For a list of supported Audit Manager Regions, see [AWS Regions and Endpoints](#) 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 assessment report destination and the KMS key used for data encryption, see [AWS Audit Manager settings](#).

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. For instructions, see [Allowing users in other accounts to use a KMS key](#) in the *AWS Key Management Service Service Developer Guide*.

Other issues to consider

Cross-account S3 buckets

Note

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 against 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 *placeholders* 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",
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:PutObjectAcl",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3::cross-account-bucket",
        "arn:aws:s3::cross-account-bucket/*"
      ]
    }
  ]
}
```

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 AWS 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 provided by AWS. 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 \(p. 109\)](#).

You can create an assessment from any standard or custom framework. For instructions on how to create and manage assessments, see [Assessments in AWS Audit Manager \(p. 33\)](#).

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 AWS Audit Manager.

Topics

- [Accessing the available frameworks in AWS Audit Manager \(p. 69\)](#)
- [Viewing the details of a framework \(p. 70\)](#)
- [Creating a custom framework \(p. 71\)](#)
- [Editing a custom framework \(p. 74\)](#)
- [Deleting a custom framework \(p. 76\)](#)
- [Supported frameworks in AWS Audit Manager \(p. 76\)](#)

Accessing the available frameworks in AWS Audit Manager

You can find a list of all the available frameworks on the **Framework library** page in AWS Audit Manager. From the framework library page, you can also [create an assessment from a framework](#), [create a custom framework](#), or [customize an existing framework](#).

To access available frameworks 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 **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 that are associated with that framework.

Viewing the details of a framework

You can open a framework and view its details at any time.

To view the details of a framework

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 standard and custom 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 in the following sections.

Sections of the framework details page

- [Framework details \(p. 70\)](#)
- [Control sets \(p. 71\)](#)
- [Tags tab \(p. 71\)](#)

Framework details

The **Framework details** dashboard provides an overview of the framework and its configuration.

It includes the following information:

1. **Framework name** – The name of the framework.
2. **Compliance type** – The compliance standard or regulation that the framework supports.
3. **Description** – A description of the framework, if one was provided.
4. **[X] automated controls** – The number of automated controls in the framework.
5. **Framework type** – Specifies whether the framework is a standard or custom framework.
6. **Control sets** – The number of control sets that are associated with the framework.
7. **Controls** – The total number of controls in the framework.
8. **Control sources** – The number of control data sources where AWS Audit Manager collects evidence from.
9. **Tags** – The tags that are associated with the framework.

If you're viewing a custom framework, the following details are also displayed:

1. **Created by** – The account that created the custom framework.

2. **Date created** – The date that the custom framework was created.
3. **Last updated** – The date when this framework was last edited.

Control sets

Under **Control sets**, the list of controls for the framework is displayed and grouped by control set.

It includes the following information:

- **Controls grouped by control sets** – The name of the control set. Select the control set name to see the full list of controls within the control set.
- **Type** – Specifies whether the control is a standard or custom control.
- **Data source** – The resource that AWS Audit Manager collects evidence from to support the requirements of the control.

Tags tab

The **Tags** tab provides an overview of the tags that are associated with the framework.

It includes the following information:

1. **Key** – The key of the tag. It might be a compliance standard, regulation, or category.
2. **Value** – The value of the tag.

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. You can customize an existing framework, or you can create a new framework from scratch.

Topics

- [Creating a new custom framework from scratch \(p. 71\)](#)
- [Customizing an existing framework \(p. 73\)](#)

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 \(p. 72\)](#)
- [Step 2: Specify the controls in the control sets \(p. 72\)](#)
- [Step 3: Review and create the framework \(p. 72\)](#)
- [What can I do next? \(p. 73\)](#)

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). The compliance standard or regulation that you enter should be a keyword such as *PCI_DSS*, *HITRUST*, or *GDPR*. 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 and can be used as a search criteria for 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 \(p. 186\)](#).
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. If you need to add more control sets than the console currently allows, we recommend that you use the [CreateAssessmentFramework](#) API that's provided by AWS Audit Manager.

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 AWS Audit Manager, and custom controls are those that you created.
3. Depending on the option that you selected in the previous step, a list of either the available standard controls or custom controls is displayed. You can browse controls from this list, or search by 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 \(p. 33\)](#).

You can also create a custom framework using an existing framework. For more information, see [Customizing an existing framework \(p. 73\)](#).

For instructions on how to edit your custom framework, see [Editing a custom framework \(p. 74\)](#).

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 according to your needs. 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 \(p. 73\)](#)
- [Step 2: Specify controls to add to control sets \(p. 74\)](#)
- [Step 3: Review and create the framework \(p. 74\)](#)
- [What can I do next? \(p. 74\)](#)

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. 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 regulation that's associated with your framework. It might be PCI_DSS, HITRUST, or GDPR. You can use this keyword to search for your framework.
5. 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 \(p. 186\)](#).
6. 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. If you need to add more control sets than the console currently allows, we recommend that you use the [CreateAssessmentFramework](#) API that's provided by AWS Audit Manager.

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. Depending on the option that you selected in the previous step, a table list of either standard controls or custom controls is displayed. You can browse control sets from this list, or search by 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 \(p. 33\)](#).

For instructions on how to edit your custom framework, see [Editing a custom framework \(p. 74\)](#).

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 \(p. 75\)](#)

- [Step 2: Edit the controls in the control set \(p. 75\)](#)
- [Step 3: Review and update the framework \(p. 76\)](#)

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**.
3. In the framework library, choose the **Custom frameworks** tab, select the framework you want to edit, and then choose **Edit**.
 - Alternatively, you can open a custom framework and choose **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 [Tags tab \(p. 71\)](#). 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. If you need to add more control sets than the console currently allows, we recommend that you use the [UpdateAssessmentFramework](#) API that's provided by AWS Audit Manager.

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. Depending on the option you selected in the previous step, a table list of either standard controls or custom controls is displayed. You can browse control sets from this list, or search by 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

Custom frameworks in AWS Audit Manager help you organize controls into control sets to suit your unique needs. You can use the framework library to find and delete an unwanted custom framework.

To delete a custom framework

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 **Custom frameworks** tab, select the framework you want to delete, and then choose **Delete**.
 - Alternatively, you can choose the name of the framework to open the framework details page, and then choose **Delete** at the top right of the page.
4. In the pop-up window, choose **Delete** to confirm deletion.

Note

Deleting a custom framework doesn't affect any existing AWS Audit Manager assessment that was created from that framework before its deletion.

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

- [AWS Audit Manager Sample Framework \(p. 77\)](#)
- [AWS Control Tower Guardrails \(p. 77\)](#)
- [AWS License Manager \(p. 78\)](#)
- [AWS Foundational Security Best Practices \(p. 79\)](#)
- [AWS Operational Best Practices \(OBP\) \(p. 79\)](#)
- [AWS Well-Architected \(p. 80\)](#)
- [CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.2.0 \(p. 81\)](#)
- [CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0 \(p. 82\)](#)
- [CIS Controls v7.1 Implementation Group 1 \(p. 83\)](#)
- [FedRAMP Moderate Baseline by Allgress \(p. 84\)](#)
- [GDPR \(p. 85\)](#)
- [Gramm-Leach-Bliley Act \(GLBA\) \(p. 100\)](#)
- [GxP 21 CFR part 11 \(p. 101\)](#)
- [GxP EU Annex 11 \(p. 101\)](#)

- [HIPAA \(p. 102\)](#)
- [HITRUST v9.4 Level 1 \(p. 103\)](#)
- [NIST 800-53 \(Rev. 5\) Low-Moderate-High \(p. 104\)](#)
- [NIST Cybersecurity Framework version 1.1 \(p. 105\)](#)
- [NIST SP 800-171 \(Rev. 2\) \(p. 106\)](#)
- [PCI DSS v3.2.1 \(p. 107\)](#)
- [SOC 2 \(p. 108\)](#)

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? \(p. 77\)](#)
- [Use AWS Audit Manager to support your audit preparation \(p. 77\)](#)

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 large 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.

Use AWS Audit Manager to support your audit preparation

You can find the *AWS Audit Manager Sample Framework* under the **Standard frameworks** tab of the [Framework library \(p. 69\)](#) in Audit Manager. You can customize this framework and its controls to support internal audits that have specific requirements.

For instructions on how to create an assessment from a framework, see [Creating an assessment \(p. 33\)](#). For instructions on how to customize a framework, see [Customizing an existing framework \(p. 73\)](#).

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? \(p. 77\)](#)
- [Use AWS Audit Manager to support your audit preparation \(p. 78\)](#)

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 Single Sign-On, 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 based on guardrails from AWS Control Tower.

Use AWS Audit Manager to support your audit preparation

AWS Audit Manager provides a prebuilt framework that structures and automates assessments for AWS Control Tower guardrails. 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 use the *AWS Control Tower Guardrails* framework in AWS Audit Manager to prepare for audits. The controls in this framework aren't intended to verify whether your systems are compliant with AWS Control Tower guardrails, and they can't guarantee that you will pass an assessment. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find the *AWS Control Tower Guardrails* framework under the **Standard frameworks** tab of the [Framework library](#) (p. 69) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment](#) (p. 33). For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

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. 78)
- [Use AWS Audit Manager to support your audit preparation](#) (p. 78)

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 your 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.

Use AWS Audit Manager to support your audit preparation

AWS Audit Manager provides a prebuilt framework that structures and automate assessments for license usage. 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 use the *AWS License Manager* framework in AWS Audit Manager to prepare for audits. The controls in this framework aren't intended to verify whether your systems are compliant with licensing rules, and they can't guarantee that you will pass a licensing usage assessment. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find the *AWS License Manager* framework under the **Standard frameworks** tab of the [Framework library](#) (p. 69) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment](#) (p. 33). For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

AWS Foundational Security Best Practices

To assist you with your audit preparation, AWS Audit Manager provides a prebuilt framework that supports the AWS Foundational Security Best Practices standard.

Topics

- [What is the AWS Foundational Security Best Practices standard? \(p. 79\)](#)
- [Use AWS Audit Manager to support your AWS Foundational Security Best Practices audit preparation \(p. 79\)](#)

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 continuously 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*.

Use AWS Audit Manager to support your AWS Foundational Security Best Practices audit preparation

You can use the *AWS Foundational Security Best Practices* framework in AWS Audit Manager to prepare for audits associated with this framework. All of its 93 controls are automated. The controls in this framework aren't intended to verify whether your systems are compliant with AWS Foundational Security Best Practices requirements, and they can't guarantee that you will pass an AWS Foundational Security Best Practices assessment.

You can find the *AWS Foundational Security Best Practices* framework under the **Standard frameworks** tab of the [Framework library](#) (p. 69) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment](#) (p. 33). For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

AWS Operational Best Practices (OBP)

AWS Audit Manager provides a prebuilt AWS Operational Best Practices 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? \(p. 80\)](#)

- [Use AWS Audit Manager to support your AWS Operational Best Practices audit preparation \(p. 80\)](#)

What is the AWS Foundational Security Best Practices standard?

You can use the *AWS Foundational Security Best Practices* to evaluate 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*.

Use AWS Audit Manager to support your AWS Operational Best Practices audit preparation

You can use the *AWS Operational Best Practices* framework in AWS Audit Manager to prepare for audits associated with this framework. All of its 52 controls are automated. The controls in this framework aren't intended to verify whether your systems are compliant with AWS Operational Best Practices, and they can't guarantee that you will pass an AWS Operational Best Practices assessment.

You can find the AWS Operational Best Practices framework under the **Standard frameworks** tab of the [Framework library \(p. 69\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 33\)](#). For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

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? \(p. 80\)](#)
- [Use AWS Well-Architected with AWS Audit Manager \(p. 80\)](#)

What is AWS Well-Architected?

AWS Well-Architected is a framework that can help you build secure, high-performing, resilient, and efficient infrastructure for your applications and workloads. Based on five pillars—operational excellence, security, reliability, performance efficiency, and cost optimization—AWS Well-Architected provides a consistent approach for you and your partners to evaluate architectures and implement designs that can scale over time.

Use AWS Well-Architected with AWS Audit Manager

The AWS Well-Architected Framework describes the key concepts, design principles, and architectural best practices for designing and running workloads in the cloud. Out of the five 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 use the *AWS Well-Architected Framework* in AWS Audit Manager to prepare for audit requirements that are associated with this framework. The framework contains 15 automated controls

and no manual controls. The controls in this framework aren't intended to guarantee that you will pass an audit that's associated with this framework. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find the *AWS Well-Architected Framework* under the **Standard frameworks** tab of the [Framework library \(p. 69\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 33\)](#). 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

To assist you with your audit preparation, 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

A more recent version of the CIS AWS Foundations Benchmark is available. For more information about this version and the frameworks that support it, see [CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0 \(p. 82\)](#).

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, providing 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 systems that are being used. *CIS Controls* are foundational best practice guidelines for an organization to follow to help protect themselves from known cyberattack vectors.

Examples

- CIS Benchmarks are very 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 tells you what should 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).

Use AWS Audit Manager to support your CIS audit preparation

You can use the *CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.2.0, Level 1* and *CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.2.0, Level 1 and 2* frameworks in AWS Audit Manager to prepare for CIS audits. The controls in these frameworks aren't intended to verify whether your systems are compliant with the CIS standard, and they can't guarantee that you will pass a CIS assessment. 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 \(p. 69\)](#) in Audit Manager.

For instructions on how to create an assessment using these frameworks, see [Creating an assessment \(p. 33\)](#). For instructions on how to customize these frameworks to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0

To assist you with your audit preparation, 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

CIS AWS Foundations Benchmark v1.3.0 is the most recent version of this benchmark. Other CIS Benchmark versions are available.

For information about 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 \(p. 81\)](#).

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, providing 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*.

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 very 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 tells you what should 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).

Use AWS Audit Manager to support your CIS audit preparation

The CIS AWS Foundations Benchmark v1.3 frameworks in AWS Audit Manager are designed to help you prepare for CIS audits. They contain the following number of controls:

- *CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0, Level 1 and 2* contains 49 automated controls and 6 manual controls
- *CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0, Level 1* contains 33 automated controls and 5 manual controls

The controls in these frameworks aren't intended to verify whether your systems are compliant with the CIS standard, and they can't guarantee that you will pass a CIS assessment. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

These frameworks provide guidance for configuring security options for a subset of AWS services with an emphasis on foundational, testable, and architecture agnostic settings. Specific AWS services in scope for these frameworks 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)

You can find the *CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0, Level 1* and *CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0, Level 1 and 2* frameworks under the **Standard frameworks** tab of the [Framework library](#) (p. 69) in Audit Manager.

For instructions on how to create an assessment using these frameworks, see [Creating an assessment](#) (p. 33). For instructions on how to customize these frameworks to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

CIS Controls v7.1 Implementation Group 1

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? \(p. 84\)](#)
- [Use AWS Audit Manager to support your CIS audit preparation \(p. 84\)](#)

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 very 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 tells you what should 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).

Use AWS Audit Manager to support your CIS audit preparation

You can use the *CIS Controls v7.1 IG1* framework in AWS Audit Manager to prepare for CIS audits. The framework contains 21 automated controls and 22 manual controls. The controls in this framework aren't intended to verify whether your systems are compliant with the CIS standard, and they can't guarantee that you will pass a CIS assessment. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find the *CIS Controls v7.1 IG1* framework under the **Standard frameworks** tab of the [Framework library \(p. 69\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 33\)](#). For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

FedRAMP Moderate Baseline by Allgress

AWS Audit Manager provides a *FedRAMP Moderate Baseline by Allgress* framework to assist you with your audit preparation.

Topics

- [What is FedRAMP? \(p. 85\)](#)

- [Use AWS Audit Manager to support your FedRAMP audit preparation \(p. 85\)](#)

What is FedRAMP?

The Federal Risk and Authorization Management Program (FedRAMP) is a US government-wide program that provides Cloud Service Providers (CSPs) a standardized approach to security assessment, authorization, and continuous monitoring for their products and services. In doing so, the program also provides assurance to federal agencies regarding the compliance of the CSPs controls related to their cloud offering.

The *FedRAMP Moderate Baseline by Allgess* framework lists the moderate impact level controls within the FedRAMP Moderate Security Controls Baseline document for CSPs that will handle government data that isn't publicly available by Allgess.

Use AWS Audit Manager to support your FedRAMP audit preparation

You can use the *FedRAMP Moderate Baseline by Allgess* framework in AWS Audit Manager to prepare for audits. The framework contains 376 automated controls and 835 manual controls. The controls in this framework aren't intended to verify whether your systems are compliant with FedRAMP, and they can't guarantee that you will pass a FedRAMP assessment. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find the *FedRAMP Moderate Baseline by Allgess* framework under the **Standard frameworks** tab of the [Framework library \(p. 69\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 33\)](#). For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

GDPR

AWS Audit Manager provides a prebuilt standard framework that supports the 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 [Use AWS Audit Manager to support your GDPR audit preparation \(p. 86\)](#).

Topics

- [What is GDPR? \(p. 85\)](#)
- [Use AWS Audit Manager to support your GDPR audit preparation \(p. 86\)](#)

What is 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) by applying a single data protection law that is binding throughout each member state.

The GDPR applies to all organizations that are established in the EU and to organizations, whether or not 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](#).

Use AWS Audit Manager to support your GDPR audit preparation

To automate evidence collection for controls under GDPR, you can use AWS Audit Manager to create custom controls for GDPR by referring to the recommended data source configuration in the following table. For instructions on how to create a custom control, see [Creating a custom control \(p. 111\)](#).

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:*:* and list all principals and services using those policies <p>When you configure the data source for the custom control, choose Automated evidence, Compliance check from AWS Config as the evidence type, and then select the following AWS Config Rules:</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>When you configure the data source for the custom control, choose Automated evidence, Compliance check from AWS Security Hub as the evidence type, and then select the following Security Hub security checks:</p> <ul style="list-style-type: none"> • 1.1 - 3.14 • Config.1
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

Control name	Control set	Recommended control data source mapping
		<p>When you configure the data source for the custom control, choose Automated evidence, Compliance check from AWS Config as the evidence type, and then select the following AWS Config Rules:</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>When you configure the data source for the custom control, choose Automated evidence, Compliance check from AWS Security Hub as the evidence type, and then select the following Security Hub security checks:</p> <ul style="list-style-type: none"> • 1.1 - 3.14 • Config.1
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 configure the data source for the custom control, choose Automated evidence, Compliance check from AWS Config as the evidence type, and then select the following AWS Config Rules:</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>When you configure the data source for the custom control, choose Automated evidence, Compliance check from AWS Security Hub as the evidence type, and then select the following Security Hub security checks:</p> <ul style="list-style-type: none"> • 1.1 - 3.14 • Config.1

Control name	Control set	Recommended control data source mapping
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 configure the data source for the custom control, choose Automated evidence, Compliance check from AWS Config as the evidence type, and then select the following AWS Config Rules:</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>When you configure the data source for the custom control, choose Automated evidence, Compliance check from AWS Security Hub as the evidence type, and then select the following Security Hub security check:</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 configure the data source for the custom control, choose Automated evidence, Compliance check from AWS Config as the evidence type, and then select the following AWS Config Rules:</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>When you configure the data source for the custom control, choose Automated evidence, Compliance check from AWS Security Hub as the evidence type, and then select the following Security Hub security check:</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 configure the data source for the custom control, choose Automated evidence, Compliance check from AWS Config as the evidence type, and then select the following AWS Config Rules:</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>When you configure the data source for the custom control, choose Automated evidence, Compliance check from AWS Security Hub as the evidence type, and then select the following Security Hub security check:</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 configure the data source for the custom control, choose Automated evidence, Compliance check from AWS Config as the evidence type, and then select the following AWS Config Rules:</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>When you configure the data source for the custom control, choose Automated evidence, Compliance check from AWS Security Hub as the evidence type, and then select the following Security Hub security check:</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 configure the data source for the custom control, choose Automated evidence, Compliance check from AWS Config as the evidence type, and then select the following AWS Config Rules:</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>When you configure the data source for the custom control, choose Automated evidence, Compliance check from AWS Security Hub as the evidence type, and then select the following Security Hub security check:</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 configure the data source for the custom control, choose Automated evidence, Compliance check from AWS Config as the evidence type, and then select the following AWS Config Rules:</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 • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK

Control name	Control set	Recommended control data source mapping
		<ul style="list-style-type: none">• 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 configure the data source for the custom control, choose Automated evidence, Compliance check from AWS Config as the evidence type, and then select the following AWS Config Rules:</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 • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK

Control name	Control set	Recommended control data source mapping
		<ul style="list-style-type: none">• 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 configure the data source for the custom control, choose Automated evidence, Compliance check from AWS Config as the evidence type, and then select the following AWS Config Rules:</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 • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED

Control name	Control set	Recommended control data source mapping
		<ul style="list-style-type: none">• 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 configure the data source for the custom control, choose Automated evidence, Compliance check from AWS Config as the evidence type, and then select the following AWS Config Rules:</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 • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED

Control name	Control set	Recommended control data source mapping
		<ul style="list-style-type: none"> • 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 \(p. 71\)](#) and [Editing a custom framework \(p. 74\)](#). You can then create an assessment from the custom GDPR framework so that AWS Audit Manager begins collecting evidence automatically for the custom controls that you added. For instructions on how to create an assessment from a framework, see [Creating an assessment \(p. 33\)](#).

Gramm-Leach-Bliley Act (GLBA)

To assist you with your audit preparation, AWS Audit Manager provides a prebuilt framework that supports the Gramm-Leach-Bliley Act (GLBA).

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.

Use AWS Audit Manager to support your Gramm-Leach-Bliley-Act 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 4 automated controls and 110 manual controls. 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.

The controls in this Audit Manager framework aren't intended to verify whether your systems are compliant with GLBA regulations. Moreover, they can't guarantee that you'll pass a GLBA assessment. 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 \(p. 69\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 33\)](#). 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

To assist you with your audit preparation, 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 \(p. 101\)](#).

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 and 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 they 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.

Use AWS Audit Manager to support your GxP audit preparation

AWS Audit Manager provides a prebuilt framework that structures and automates assessments for GxP regulations based on AWS best practices. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped according to GxP requirements.

You can use the *GxP 21 CFR Part 11* framework in AWS Audit Manager to prepare for audits. The controls in this framework aren't intended to verify whether your systems are compliant with GxP regulations. Moreover, they can't guarantee that you will pass a GxP assessment. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find the *GxP 21 CFR Part 11* framework under the **Standard frameworks** tab of the [Framework library \(p. 69\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 33\)](#). For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

GxP EU Annex 11

To assist you with your audit preparation, AWS Audit Manager provides a prebuilt framework that supports GxP EU Annex 11 regulations that are 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 \(p. 101\)](#).

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 forth by the Commission of the European Communities 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.

Use AWS Audit Manager with the GxP EU Annex 11 framework

You can use *The GxP EU Annex 11 framework* in AWS Audit Manager to prepare for audits that are associated with this framework. It contains 19 automated controls and 13 manual controls. The controls in this framework aren't intended to verify whether your systems are compliant with the GxP EU Annex 11 requirements. Moreover, they can't guarantee that you will pass a GxP EU Annex 11 assessment. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find the *GxP EU Annex 11 framework* under the **Standard frameworks** tab of the [Framework library \(p. 69\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 33\)](#). For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

HIPAA

AWS Audit Manager provides a prebuilt framework that supports HIPAA rules to assist you with your audit preparation.

Topics

- [What is HIPAA? \(p. 102\)](#)
- [Use AWS Audit Manager to support your HIPAA audit preparation \(p. 103\)](#)

What is HIPAA?

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 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 US 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.

Use AWS Audit Manager to support your HIPAA audit preparation

AWS Audit Manager provides a prebuilt framework that structures and automates assessments for the HIPAA compliance standard based on AWS best practices. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped according to HIPAA requirements. You can also customize this framework and its controls to support internal audits with unique requirements.

You can use the *HIPAA* framework in AWS Audit Manager to prepare for HIPAA audits. The controls in this framework aren't intended to verify whether your systems are compliant with the HIPAA standard. They can neither replace internal efforts nor guarantee that you will pass a HIPAA assessment. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection. Moreover, it doesn't check procedural controls that require manual evidence collection.

You can find the HIPAA framework under the **Standard frameworks** tab of the [Framework library](#) (p. 69) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment](#) (p. 33). For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

HITRUST v9.4 Level 1

AWS Audit Manager provides a prebuilt framework that supports HITRUST to assist you with your audit preparation.

What is HITRUST?

The [Health Information Trust Alliance](#) (HITRUST) Common Security Framework (CSF), in their own words, "is a certifiable framework that provides organizations with a comprehensive, flexible, and efficient approach to regulatory compliance and risk management. Developed in collaboration with healthcare and information security professionals, the HITRUST CSF rationalizes healthcare-relevant regulations and standards into a single overarching security framework."

The HITRUST CSF serves to unify security controls from federal law (such as HIPAA and HITECH), state law (such as the Massachusetts [Standards for the Protection of Personal Information of Residents of the Commonwealth](#)), and non-governmental frameworks (such as the PCI Security Standards Council) into a single framework that's tailored for healthcare needs.

AWS provides a reliable, scalable, and inexpensive computing platform that can support the applications of healthcare customers in a manner consistent with HIPAA, HITECH, and HITRUST CSF.

Use AWS Audit Manager to support your HITRUST audit preparation

AWS Audit Manager provides a prebuilt framework that structures and automates assessments for the HITRUST compliance standard, based on AWS best practices. This framework includes a prebuilt collection of controls with descriptions and testing procedures. These controls are grouped according to HITRUST requirements.

You can use the *HITRUST v9.4 - Level 1* framework in AWS Audit Manager to prepare for HITRUST audits. The controls in this framework aren't intended to verify whether your systems are compliant with the HITRUST standard. Moreover, they can't guarantee that you will pass a HITRUST assessment. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find the *HITRUST v9.4 - Level 1* framework under the **Standard frameworks** tab of the [Framework library](#) (p. 69) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment](#) (p. 33). For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

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. 106).
- For information about the Audit Manager framework that supports the *NIST Cybersecurity Framework*, see [NIST Cybersecurity Framework version 1.1](#) (p. 105).

Topics

- [What is NIST 800-53?](#) (p. 104)
- [Use AWS Audit Manager to support your NIST audit preparation](#) (p. 104)

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 remove a major challenge to US industrial competitiveness at the time—a second-rate measurement infrastructure that lagged behind the capabilities of the United Kingdom, Germany, and other economic powers.

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, based on the security category and impact level of the system (low, moderate, or high), and 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.

Use AWS Audit Manager to support your NIST audit preparation

You can use the *NIST 800-53 (Rev. 5) Low-Moderate-High* framework in AWS Audit Manager to prepare for NIST audits. The framework contains 225 automated controls and 782 manual controls. The controls

in this framework aren't intended to verify whether your systems are compliant with the NIST standard. Moreover, they can't guarantee that you will pass a NIST assessment. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

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](#).

You can find the *NIST 800-53 (Rev. 5) Low-Moderate-High* framework under the **Standard frameworks** tab of the [Framework library](#) (p. 69) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment](#) (p. 33). For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

NIST Cybersecurity Framework version 1.1

To assist you with your audit preparation, 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. 104).
- For information about the Audit Manager framework that supports *NIST SP 800-171 (Rev. 2)*, see [NIST SP 800-171 \(Rev. 2\)](#) (p. 106).

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 remove a major challenge to U.S. industrial competitiveness at the time—a second-rate measurement infrastructure that lagged behind the capabilities of the United Kingdom, Germany, and other economic powers.

The United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing 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. Cybersecurity can be an important and amplifying component of an organization's overall risk management.

The NIST Cybersecurity Framework (CSF) is supported by governments and industries worldwide as a recommended baseline for use by any organization, regardless of its 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.

Use AWS Audit Manager to support your NIST audit preparation

You can use the *NIST Cybersecurity Framework version 1.1* framework in AWS Audit Manager to prepare for NIST audits. 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. The controls that are offered by Audit Manager aren't intended to verify whether your systems are compliant with the NIST Cybersecurity Framework. Moreover, they can't guarantee that you will pass a NIST Cybersecurity assessment. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find *NIST Cybersecurity Framework version 1.1* under the **Standard frameworks** tab of the [Framework library](#) (p. 69) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment](#) (p. 33). For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

NIST SP 800-171 (Rev. 2)

To assist you with your audit preparation, 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. 104).
- For information about the Audit Manager framework that supports *NIST Cybersecurity Framework version 1.1*, see [NIST Cybersecurity Framework version 1.1](#) (p. 105).

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, and 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 has released an array of standards and publications to strengthen cybersecurity resilience in both 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 are designed to 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.

Use AWS Audit Manager to support your NIST audit preparation

You can use the *NIST SP 800-171 Rev. 2* framework in AWS Audit Manager to prepare for NIST audits. It contains 66 automated controls and 58 manual controls. The controls offered in this framework aren't intended to verify whether your systems are compliant with NIST 800-171, and they can't guarantee that you will pass a NIST assessment. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find *NIST SP 800-171 Rev. 2* under the **Standard frameworks** tab of the [Framework library \(p. 69\)](#) in Audit Manager.

For information about how to create an assessment using this framework, see [Creating an assessment \(p. 33\)](#). For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

PCI DSS v3.2.1

AWS Audit Manager provides a prebuilt framework that supports PCI DSS v3.2.1 to assist you with audit preparation.

Topics

- [What is PCI DSS? \(p. 107\)](#)
- [Use AWS Audit Manager to support your PCI DSS audit preparation \(p. 107\)](#)

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, 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, which 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](#).

Use AWS Audit Manager to support your PCI DSS audit preparation

AWS Audit Manager provides a prebuilt framework that structures and automates assessments to support the PCI DSS compliance standard, based on AWS best practices. This framework includes a prebuilt collection of controls with descriptions and testing procedures, which are grouped according to PCI DSS requirements. The framework contains 152 automated controls and 510 manual controls. You can also customize this framework and its controls to support internal audits with unique requirements.

You can use the *PCI DSS V3.2.1* framework in AWS Audit Manager to prepare for PCI DSS audits. The controls in this framework aren't intended to verify whether your systems are compliant with the PCI DSS standard. Moreover, they can't guarantee that you will pass a PCI DSS assessment. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find the *PCI DSS V3.2.1* framework under the **Standard frameworks** tab of the [Framework library \(p. 69\)](#) in Audit Manager.

For information about how to create an assessment using this framework, see [Creating an assessment \(p. 33\)](#). For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

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 to assist you with your audit preparation.

Topics

- [What is SOC 2? \(p. 108\)](#)
- [Use AWS Audit Manager to support your audit preparation \(p. 108\)](#)

What is SOC 2?

System and Organization Controls (SOC), defined by the [American Institute of Certified Public Accountants \(AICPA\)](#), is the name of a suite of reports 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](#).

Use AWS Audit Manager to support your audit preparation

AWS Audit Manager provides a prebuilt framework that structures and automates assessments based on AWS best practices. This framework includes a prebuilt collection of controls with descriptions and testing procedures. You can also customize this framework and its controls to support internal audits with unique requirements.

SOC 2 is an auditing procedure that ensures a company's data is securely managed protecting the interests of the organization and privacy of clients. You can use the AWS Audit Manager framework for SOC 2 to prepare for audits. The controls in this AWS Audit Manager framework aren't intended to verify whether your systems are compliant. Moreover, they can't guarantee that you will pass an assessment. AWS Audit Manager doesn't automatically check procedural controls that require manual evidence collection.

You can find the SOC 2 framework under the **Standard frameworks** tab of the [Framework library \(p. 69\)](#) in Audit Manager.

For instructions on how to create an assessment using this framework, see [Creating an assessment \(p. 33\)](#). For instructions on how to customize this framework to support your specific requirements, see [Customizing an existing framework](#) and [Customizing an existing control](#).

Control library

The *control library* is the central place from which you can manage the controls used in AWS Audit Manager frameworks. You can go to the control library at any time by choosing **Control library** in the left navigation pane in the Audit Manager console.

The control library contains a catalog of standard and custom controls.

- **Standard controls** are predefined controls 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 fits your unique requirements.
- **Custom controls** are customized controls that you own and define. With a custom control, you can specify from which data sources you want to collect evidence. 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 \(p. 69\)](#). To learn more about how to create an assessment from an Audit Manager framework, see [Assessments in AWS Audit Manager \(p. 33\)](#).

This section provides information about how you can create and manage a custom control in AWS Audit Manager.

Topics

- [Accessing the available controls in AWS Audit Manager \(p. 109\)](#)
- [Viewing the details of a control \(p. 110\)](#)
- [Creating a custom control \(p. 111\)](#)
- [Editing a custom control \(p. 117\)](#)
- [Deleting a custom control \(p. 119\)](#)
- [Changing the evidence collection frequency for a control \(p. 119\)](#)
- [Supported control data sources for automated evidence \(p. 122\)](#)

Accessing the available controls in AWS Audit Manager

You can find a list of all available controls on the **Control library** page in AWS Audit Manager. From the control library page, you can also [create a custom control](#) or [customize an existing control](#).

To access available controls 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 **Control library**.
3. Select the **Standard controls** tab or the **Custom controls** tab to browse the available standard and custom controls.

4. Select any control name to view the details for that control.

Viewing the details of a control

You can open a control and view its details at any time.

To view the details of a control

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the left navigation pane, choose **Control library** to see a list of available controls.
3. Select the **Standard controls** tab or the **Custom controls** tab to browse the available standard and custom controls.
4. Select any control name to view the details for that control.

When you open a control, you will see a summary page. The sections of this page and their contents are described below.

Sections of the control details page

- [Summary \(p. 110\)](#)
- [Control details tab \(p. 110\)](#)
- [Tags tab \(p. 111\)](#)

Summary

The **Summary** section provides an overview of the control. It includes the following information:

1. **Control name** – The name given to the control.
2. **Control type** – Specifies whether the control is a standard or custom control.
3. **Control sources** – The number of data sources for this control.
4. **Tags** – The number of tags associated with this control.

Control details tab

- The **Control details** section provides an overview of the control. It includes the following information:
 - **Control name** – The name given to the control.
 - **Control description** – The description of the control.
- The **Testing information** section provides a description of the recommended testing procedures for this control, such as a list of associated AWS Security Hub security checks or AWS Config rules.
- The **Data sources** section provides an overview of the data source for the control. It includes the following information:
 - **Name** – The name of the data source from which AWS Audit Manager collects evidence
 - **Data source** – The name of the AWS service that contains this data.
 - **Attribute** – The associated attribute value for retrieving the data from the data source. For example, this can be the parameter attribute used when making a describe API call to an AWS service.
 - **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 \(p. 7\)](#).

- The **Action plan** section describes the recommended actions to carry out if the control is not fulfilled. It includes the following information:
 - **Title** – The title of the action plan.
 - **Action plan instructions** – The specific actions to carry out if the control is not fulfilled.

Tags tab

The **Tags** tab provides an overview of the tags associated with the control.

It includes the following information:

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

Creating a custom control

The control library is the central place from which you can manage the controls used in AWS Audit Manager frameworks. The control library contains a catalog of standard controls and custom controls.

There are two ways to create a custom control. You can customize an existing control, or you can create a new control from scratch.

Topics

- [Creating a custom control from scratch \(p. 111\)](#)
- [Customizing an existing control \(p. 114\)](#)

Creating a custom control from scratch

You can use the control library in AWS Audit Manager to create a new custom control from scratch by performing the following steps.

Topics

- [Step 1: Specify control details \(p. 111\)](#)
- [Step 2: Configure data sources for this control \(p. 112\)](#)
- [Step 3 \(Optional\): Define an action plan \(p. 113\)](#)
- [Step 4: Review and create the control \(p. 114\)](#)
- [What can I do next? \(p. 114\)](#)

Step 1: Specify control details

First, you must specify the details for 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 left navigation pane, choose **Control library**, and choose **Create custom control**.
3. Under **Control details**, enter a name and description for your control.

4. Under **Testing information**, enter the recommended testing information. This should include the steps that you would follow to determine if the control has been satisfied.
5. Under **Tags**, choose **Add new tag** to associate a tag with your control. You can specify a key for each tag that best describes the compliance framework that this control will support.

The tag key is mandatory and can be used as a search criteria when you search for this control in the control library. For more information about tags in AWS Audit Manager, see [Tagging AWS Audit Manager resources \(p. 186\)](#).

6. Choose **Next**.

Step 2: Configure data sources for this control

You can specify a data source to determine from where you want AWS Audit Manager to collect evidence for this control. You can add up to 10 data sources to a new custom control in Audit Manager.

To configure data sources for this control

1. In the data source box under **Select evidence collection method**, select one of the following options.
 - **Automated evidence** – Select this option for system evidence that you want Audit Manager to automatically collect for you.
 - **Manual evidence** – Select this option for evidence that Audit Manager can't collect automatically.

For example: if the control is a procedural control that covers team organization, you can choose **Manual evidence**. When this control is active in an assessment, you can then upload a copy of your organization chart manually as evidence to support the control.
2. (For automated evidence) Under **Select an evidence type by mapping to a data source**, select one of the following data sources for your custom control.

Data source	Description	Evidence collection frequency	To use this data source...	When this control is active in an assessment...
User activity logs from AWS CloudTrail	Tracks a particular user activity that is needed in your audit.	Continuous	Choose from the dropdown list of keywords to search for in CloudTrail logs.	Audit Manager assesses your CloudTrail logs, filters the relevant logs based on your keyword, and then converts processed logs to User activity evidence.
Compliance checks for security findings from AWS Security Hub	Captures snapshots of your resource security posture in addition to configuration changes checked	Based on the schedule of the Security Hub check	Choose from the dropdown list of Security Hub checks supported by Audit Manager . Custom checks aren't currently supported.	Audit Manager assesses the Security Hub findings that are associated with this Security Hub check, and then converts the processed data to Compliance check evidence.

Data source	Description	Evidence collection frequency	To use this data source...	When this control is active in an assessment...
	by Security Hub.			
Compliance checks for resource configurations from AWS Config	Captures snapshots of your resource security posture in addition to configuration changes evaluated by AWS Config.	Based on the triggers defined in the AWS Config rule	Choose from the dropdown list of AWS Config rules supported by Audit Manager . Custom rules aren't currently supported.	Audit Manager assesses the CloudTrail logs that are associated with this AWS Config rule evaluation, and then converts the processed data to Compliance check evidence.
Configuration snapshots from AWS API calls	Takes a snapshot of your resource configuration directly via an API call to the specified AWS service.	Daily, weekly, or monthly	Choose from the dropdown list of APIs supported by Audit Manager , and specify your preferred frequency.	Audit Manager makes the API call based on the defined frequency, assesses the results from the API call, and then converts the results to Configuration data evidence.

- (Optional) Under **Troubleshooting description**, enter the suggested actions to take if no evidence is collected from the control data source.
- To add another data source to the control, choose **Add data source** at the bottom of the page and repeat steps 1-3.
- To remove an unwanted data source from the control, choose **Remove** at the top of the data source box.
- When you are finished, choose **Next**.

Tip

If you aren't sure how to configure the control and you want to ask a subject matter expert for help, we suggest that you choose **Manual evidence** for now. You can save the control and add it to a framework at this time, and then then edit the control at a later date. To learn more about how to edit a control, see [Editing a custom control \(p. 117\)](#).

Step 3 (Optional): Define an action plan

Specify the actions to take if this control is not fulfilled.

To define an action plan

- Under **Title**, enter a descriptive title for the action plan.

2. Under **Action plan instructions**, enter detailed instructions for your action plan.
3. Choose **Next**.

Step 4: Review and create the control

Review the information for your control. To change the information for a step, choose **Edit**.

When you are finished, choose **Create custom control**.

What can I do next?

After you create your new custom control, you can add it to a custom framework. To learn more, see [Creating a custom framework \(p. 71\)](#) or [Editing a custom framework \(p. 74\)](#).

After you've added your custom control to a custom framework, you can create an assessment from that custom framework and begin collecting evidence. To learn more, see [Creating an assessment \(p. 33\)](#).

Customizing an existing control

The control library in AWS Audit Manager contains a catalog of standard controls and also custom controls that you have created. Instead of creating a custom control from scratch, you can customize an existing control and modify it as needed to suit your specific audit requirements.

Perform the following steps to customize a control.

Topics

- [Step 1: Specify control details \(p. 114\)](#)
- [Step 2: Configure data sources for this control \(p. 114\)](#)
- [Step 3: \(Optional\): Define an action plan \(p. 116\)](#)
- [Step 4: Review and create the control \(p. 116\)](#)
- [What can I do next? \(p. 116\)](#)

Step 1: Specify control details

The control details are carried over 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**, review the name and description for your control, and modify them as needed.
6. Under **Testing information**, review the recommended testing information, and modify it as needed.
7. Under **Tags**, review and modify the tags as needed.
8. Choose **Next**.

Step 2: Configure data sources for this control

Data sources are carried over from the original control. You can modify the existing data sources, add more data sources, or remove existing control data sourced as needed.

To configure data sources for this control

1. In the data source box under **Select evidence collection method**, review the current selection and modify it if needed.
 - **Automated evidence** – Select this option for system evidence that you want Audit Manager to automatically collect for you.
 - **Manual evidence** – Select this option for evidence that Audit Manager can't collect automatically.

For example: if the control is a procedural control that covers team organization, you can choose **Manual evidence**. When this control is active in an assessment, you can then upload a copy of your organization chart manually as evidence to support the control.
2. (For automated evidence) Under **Select an evidence type by mapping to a data source**, review the currently selected data source and modify as needed. You can choose from the following data sources.

Data source	Description	Evidence collection frequency	To use this data source...	When this control is active in an assessment...
User activity logs from AWS CloudTrail	Tracks a particular user activity that is needed in your audit.	Continuous	Choose from the dropdown list of keywords to search for in CloudTrail logs.	Audit Manager assesses your CloudTrail logs, filters the relevant logs based on your keyword, and then converts processed logs to User activity evidence.
Compliance checks for security findings from AWS Security Hub	Captures snapshots of your resource security posture in addition to configuration changes checked by Security Hub.	Based on the schedule of the Security Hub check	Choose from the dropdown list of Security Hub checks supported by Audit Manager . Custom checks aren't currently supported.	Audit Manager assesses the Security Hub findings that are associated with this Security Hub check, and then converts the processed data to Compliance check evidence.
Compliance checks for resource configurations from AWS Config	Captures snapshots of your resource security posture in addition to configuration changes evaluated	Based on the triggers defined in the AWS Config rule	Choose from the dropdown list of AWS Config rules supported by Audit Manager . Custom rules aren't currently supported.	Audit Manager assesses the CloudTrail logs that are associated with this AWS Config rule evaluation, and then converts the processed data to Compliance check evidence.

Data source	Description	Evidence collection frequency	To use this data source...	When this control is active in an assessment...
	by AWS Config.			
Configuration snapshots from AWS API calls	Takes a snapshot of your resource configuration directly via an API call to the specified AWS service.	Daily, weekly, or monthly	Choose from the dropdown list of APIs supported by Audit Manager , and specify your preferred frequency.	Audit Manager makes the API call based on the defined frequency, assesses the results from the API call, and then converts the results to Configuration data evidence.

3. (Optional) Under **Troubleshooting description**, make any necessary changes to the suggested actions to take if no evidence is collected from the control data source.
4. To add another data source to the control, choose **Add data source** at the bottom of the page.
5. To remove an unwanted data source from the control, choose **Remove** at the top of the data source box.
6. Choose **Next**.

Tip

If you aren't sure how to configure the control and you want to ask a subject matter expert for help, we suggest that you choose **Manual evidence** for now. You can save the control and add it to a framework at this time, and then then edit the control at a later date. To learn more about how to edit a control, see [Editing a custom control \(p. 117\)](#).

Step 3: (Optional): Define an action plan

The action plan is carried over from the original control. Review and customize the actions to take if this control is not fulfilled.

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 your control. To change the information for a step, choose **Edit**. When you are finished, choose **Create custom control**.

What can I do next?

After you create your new custom control, you can add it to a custom framework. To learn more, see [Creating a custom framework \(p. 71\)](#) or [Editing a custom framework \(p. 74\)](#).

After you add your custom control to a custom framework, you can create an assessment from that custom framework and begin collecting evidence. To learn more, see [Creating an assessment \(p. 33\)](#).

If you need to edit your custom control, see [Editing a custom control \(p. 117\)](#).

Editing a custom control

You can edit a custom control in AWS Audit Manager by performing the following steps.

Topics

- [Step 1: Edit control details \(p. 117\)](#)
- [Step 2: Edit data sources for this control \(p. 117\)](#)
- [Step 3: \(Optional\) Edit an action plan \(p. 119\)](#)
- [Step 4: Review and update the control \(p. 119\)](#)

Step 1: Edit control details

Start by editing and reviewing 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 name and description for your control 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 \(p. 111\)](#), where you can view and edit the tags associated with the control.

Step 2: Edit data sources for this control

Edit the control data sources, add more data sources, or remove data sources.

To edit data sources for this control

1. In the data source box under **Select evidence collection method**, review the current selection and modify it as needed.
 - **Automated evidence** – Select this option for system evidence that you want Audit Manager to automatically collect for you.
 - **Manual evidence** – Select this option for evidence that you will upload manually.

For example: if the control is a procedural control that covers team organization, you can choose **Manual evidence**. When this control is active in an assessment, you can then upload a copy of your organization chart manually as evidence to support the control.

2. (For automated evidence) Under **Select an evidence type by mapping to a data source**, review the currently selected data source and modify as needed. You can choose from the following data sources.

Data source	Description	Evidence collection frequency	To use this data source...	When this control is active in an assessment...
User activity logs from AWS CloudTrail	Tracks a particular user activity that is needed in your audit.	Continuous	Choose from the dropdown list of keywords to search for in CloudTrail logs.	Audit Manager assesses your CloudTrail logs, filters the relevant logs based on your keyword, and then converts processed logs to User activity evidence.
Compliance checks for security findings from AWS Security Hub	Captures snapshots of your resource security posture in addition to configuration changes checked by Security Hub.	Based on the schedule of the Security Hub check	Choose from the dropdown list of Security Hub checks supported by Audit Manager . Custom checks aren't currently supported.	Audit Manager assesses the Security Hub findings that are associated with this Security Hub check, and then converts the processed data to Compliance check evidence.
Compliance checks for resource configurations from AWS Config	Captures snapshots of your resource security posture in addition to configuration changes evaluated by AWS Config.	Based on the triggers defined in the AWS Config rule	Choose from the dropdown list of AWS Config rules supported by Audit Manager . Custom rules aren't currently supported.	Audit Manager assesses the CloudTrail logs that are associated with this AWS Config rule evaluation, and then converts the processed data to Compliance check evidence.
Configuration snapshots from AWS API calls	Takes a snapshot of your resource configuration directly via an API call to the specified AWS service.	Daily, weekly, or monthly	Choose from the dropdown list of APIs supported by Audit Manager , and specify your preferred frequency.	Audit Manager makes the API call based on the defined frequency, assesses the results from the API call, and then converts the results to Configuration data evidence.

3. (Optional) Under **Troubleshooting description**, make any necessary changes to the suggested actions.
4. To add another data source to the control, choose **Add data source** at the bottom of the page.
5. To remove an unwanted data source from the control, choose **Remove** at the top of the data source box.
6. Choose **Next**.

Step 3: (Optional) Edit an action plan

Review and edit the optional action plan as needed.

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 your control. To change the information for a step, choose **Edit**.

When you are 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 *Configuration data from AWS API calls* as the data source, 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 a custom control. After you delete a control, it no longer appears in the control library. The control is also removed from any associated frameworks or assessments.

To delete a custom control

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.

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's being collected for your control.

- For **Configuration snapshots from 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 **Compliance checks for resource configurations from AWS Config**, Audit Manager collects evidence from AWS Config. The evidence collection frequency follows the triggers defined in your AWS Config Rules.
- For **Compliance checks for security findings from AWS Security Hub**, Audit Manager collects evidence from Security Hub. The evidence collection frequency follows the schedule of your Security Hub checks.
- For **User activity logs from 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, and how to change it (if applicable).

Topics

- [Configuration snapshots from AWS API calls \(p. 120\)](#)
- [Compliance checks for resource configurations from AWS Config \(p. 121\)](#)
- [Compliance checks for security findings from Security Hub \(p. 121\)](#)
- [User activity logs from AWS CloudTrail \(p. 121\)](#)

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 your custom control uses API calls as a data source, you can change the evidence collection frequency in AWS Audit Manager by performing the following 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 left 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. In the data source box, ensure that you have selected **Automated evidence** and **Configuration snapshots from AWS API calls**, and verify that the name of the API call is the one that you want to change the frequency for.
6. Under **Custom control 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 for the custom control.
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 your custom control. To change the information for a step, choose **Edit**.
11. When you are finished, choose **Save changes**.

After you edit a control with *Configuration data from AWS API calls* as the data source, the changes take effect at 00:00 UTC the following day in all active assessments that include the control.

Compliance checks for resource configurations from AWS Config

Note

The following applies to both standard and custom controls that use AWS Config Rules as a data source.

If your control uses AWS Config as a data source, you can't change the evidence collection frequency directly in AWS Audit Manager. This is because the evidence collection frequency follows the triggers defined in your AWS Config Rules.

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 for security findings from Security Hub

Note

The following applies to both standard and custom controls that use Security Hub checks as a data source.

If your control uses Security Hub as a data source, you can't change the evidence collection frequency directly in AWS Audit Manager. This is because the evidence collection frequency follows the schedule of your 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 does not 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 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. AWS Audit Manager collects this evidence type from CloudTrail in a continuous manner. The evidence collection frequency is continuous because user activity can happen at any time of the day.

Supported control data sources for automated evidence

When you configure a custom control in AWS Audit Manager, you can choose to collect automated evidence for that control. You can select one of the following four types of control data sources for automated evidence:

- User activity logs from AWS CloudTrail
- Compliance checks for security findings from AWS Security Hub
- Compliance checks for resource configurations from AWS Config
- Configuration data from AWS API calls

The following topics list the AWS Security Hub checks, AWS Config rules, and AWS API calls that are supported by AWS Audit Manager.

Topics

- [AWS Config rules supported by AWS Audit Manager \(p. 122\)](#)
- [AWS Security Hub checks supported by AWS Audit Manager \(p. 126\)](#)
- [API calls supported by AWS Audit Manager \(p. 127\)](#)
- [AWS CloudTrail event names supported by AWS Audit Manager \(p. 128\)](#)

AWS Config rules supported by AWS Audit Manager

AWS Audit Manager allows you to capture AWS Config findings as evidence by specifying an AWS Config rule when you configure a control.

The following AWS Config Rules are supported by AWS Audit Manager. Custom AWS Config rules are not yet supported. For more information about any of the rules listed below, choose an item from the list or see [AWS Config Managed Rules](#) in the *AWS Config User Guide*.

Supported AWS Config Rules

- [IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS](#)
- [IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS](#)
- [ACCESS_KEYS_ROTATED](#)
- [ACCOUNT_PART_OF_ORGANIZATIONS](#)
- [ACM_CERTIFICATE_EXPIRATION_CHECK](#)
- [ALB_HTTP_DROP_INVALID_HEADER_ENABLED](#)
- [ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK](#)
- [ALB_WAF_ENABLED](#)
- [API_GW_CACHE_ENABLED_AND_ENCRYPTED](#)
- [API_GW_ENDPOINT_TYPE_CHECK](#)
- [API_GW_EXECUTION_LOGGING_ENABLED](#)
- [APPROVED_AMIS_BY_ID](#)
- [APPROVED_AMIS_BY_TAG](#)
- [AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED](#)
- [CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK](#)
- [CLOUDFORMATION_STACK_NOTIFICATION_CHECK](#)

- CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED
- CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED
- CLOUDFRONT_ORIGIN_FAILOVER_ENABLED
- CLOUDFRONT_SNI_ENABLED
- CLOUDFRONT_VIEWER_POLICY_HTTPS
- CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED
- CLOUD_TRAIL_ENABLED
- CLOUD_TRAIL_ENCRYPTION_ENABLED
- CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED
- CLOUDTRAIL_S3_DATAEVENTS_ENABLED
- CLOUDTRAIL_SECURITY_TRAIL_ENABLED
- CLOUDWATCH_ALARM_ACTION_CHECK
- CLOUDWATCH_ALARM_RESOURCE_CHECK
- CLOUDWATCH_ALARM_SETTINGS_CHECK
- CLOUDWATCH_LOG_GROUP_ENCRYPTED
- CMK_BACKING_KEY_ROTATION_ENABLED
- CODEBUILD_PROJECT_ENVVAR_AWSCRED_CHECK
- CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK
- CODEPIPELINE_DEPLOYMENT_COUNT_CHECK
- CODEPIPELINE_REGION_FANOUT_CHECK
- 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_PITR_ENABLED
- DYNAMODB_TABLE_ENCRYPTED_KMS
- DYNAMODB_TABLE_ENCRYPTION_ENABLED
- DYNAMODB_THROUGHPUT_LIMIT_CHECK
- EBS_IN_BACKUP_PLAN
- EFS_IN_BACKUP_PLAN
- EC2_EBS_ENCRYPTION_BY_DEFAULT
- EBS_OPTIMIZED_INSTANCE
- EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK
- EC2_INSTANCE_DETAILED_MONITORING_ENABLED
- EC2_INSTANCE_MANAGED_BY_SSM
- EC2_INSTANCE_NO_PUBLIC_IP
- INSTANCES_IN_VPC
- 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_SECURITY_GROUP_ATTACHED_TO_ENI
- EC2_STOPPED_INSTANCE
- EC2_VOLUME_INUSE_CHECK
- EFS_ENCRYPTED_CHECK
- EIP_ATTACHED
- ELASTICSEARCH_ENCRYPTED_AT_REST
- ELASTICSEARCH_IN_VPC_ONLY
- ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK
- EC2_IMDSV2_CHECK
- EKS_ENDPOINT_NO_PUBLIC_ACCESS
- EKS_SECRETS_ENCRYPTED
- ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- ELB_TLS_HTTPS_LISTENERS_ONLY
- ELB_ACM_CERTIFICATE_REQUIRED
- ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK
- ELB_DELETION_PROTECTION_ENABLED
- ELB_LOGGING_ENABLED
- ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK
- EMR_KERBEROS_ENABLED
- EMR_MASTER_NO_PUBLIC_IP
- ENCRYPTED_VOLUMES
- FMS_SECURITY_GROUP_AUDIT_POLICY_CHECK
- FMS_SECURITY_GROUP_CONTENT_CHECK
- FMS_SECURITY_GROUP_RESOURCE_ASSOCIATION_CHECK
- FMS_SHIELD_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK
- GUARDDUTY_ENABLED_CENTRALIZED
- GUARDDUTY_NON_ARCHIVED_FINDINGS
- IAM_NO_INLINE_POLICY_CHECK
- IAM_GROUP_HAS_USERS_CHECK
- IAM_PASSWORD_POLICY
- IAM_POLICY_BLACKLISTED_CHECK
- IAM_POLICY_IN_USE
- IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_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
- 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
- MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS
- MULTI_REGION_CLOUD_TRAIL_ENABLED
- RDS_CLUSTER_DELETION_PROTECTION_ENABLED
- RDS_INSTANCE_DELETION_PROTECTION_ENABLED
- RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED
- RDS_LOGGING_ENABLED
- REDSHIFT_BACKUP_ENABLED
- RDS_IN_BACKUP_PLAN
- RDS_SNAPSHOT_ENCRYPTED
- REDSHIFT_REQUIRE_TLS_SSL
- RDS_ENHANCED_MONITORING_ENABLED
- RDS_INSTANCE_PUBLIC_ACCESS_CHECK
- RDS_MULTI_AZ_SUPPORT
- RDS_SNAPSHOTS_PUBLIC_PROHIBITED
- RDS_STORAGE_ENCRYPTED
- REDSHIFT_CLUSTER_CONFIGURATION_CHECK
- REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK
- REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK
- REQUIRED_TAGS
- RESTRICTED_INCOMING_TRAFFIC
- INCOMING_SSH_DISABLED
- ROOT_ACCOUNT_HARDWARE_MFA_ENABLED
- ROOT_ACCOUNT_MFA_ENABLED
- S3_BUCKET_DEFAULT_LOCK_ENABLED
- S3_DEFAULT_ENCRYPTION_KMS
- SECURITYHUB_ENABLED
- SNS_ENCRYPTED_KMS
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS
- S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED
- S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE
- S3_BUCKET_LOGGING_ENABLED
- S3_BUCKET_POLICY_GRANTEE_CHECK
- 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
- SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS
- SECRETSMANAGER_ROTATION_ENABLED_CHECK

- [SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK](#)
- [SERVICE_VPC_ENDPOINT_ENABLED](#)
- [SHIELD_ADVANCED_ENABLED_AUTORENEW](#)
- [SHIELD_DRT_ACCESS](#)
- [VPC_DEFAULT_SECURITY_GROUP_CLOSED](#)
- [VPC_FLOW_LOGS_ENABLED](#)
- [VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS](#)
- [VPC_VPN_2_TUNNELS_UP](#)
- [WAF_CLASSIC_LOGGING_ENABLED](#)
- [WAFV2_LOGGING_ENABLED](#)

AWS Security Hub checks supported by AWS Audit Manager

AWS Audit Manager allows you to capture Security Hub findings as evidence by specifying a Security Hub check when you configure a control.

The following Security Hub checks are supported by AWS Audit Manager. Custom AWS Security Hub checks are not yet supported.

For more information about any of the Security Hub checks listed following, choose an item in the table or see [Security standards and controls in AWS Security Hub](#) in the *AWS Security Hub User Guide*.

CIS Foundation Benchmark	PCI DSS	AWS Foundational Security Best Practices
<ul style="list-style-type: none"> • 1.1 • 1.2 • 1.3 • 1.4 • 1.5 • 1.6 • 1.7 • 1.8 • 1.9 • 1.10 • 1.11 • 1.12 • 1.13 • 1.14 • 1.16 • 1.20 • 1.22 • 2.1 • 2.2 • 2.3 • 2.4 	<ul style="list-style-type: none"> • PCI.AutoScaling.1 • PCI.CloudTrail.1 • PCI.CloudTrail.2 • PCI.CloudTrail.3 • PCI.CloudTrail.4 • PCI.CodeBuild.1 • PCI.CodeBuild.2 • PCI.Config.1 • PCI.CW.1 • PCI.DMS.1 • PCI.EC2.1 • PCI.EC2.2 • PCI.EC2.3 • PCI.EC2.4 • PCI.EC2.5 • PCI.EC2.6 • PCI.ELBV2.1 • PCI.ES.1 • PCI.ES.2 • PCI.GuardDuty.1 • PCI.IAM.1 	<ul style="list-style-type: none"> • ACM.1 • AutoScaling.1 • CloudTrail.1 • CloudTrail.2 • CodeBuild.1 • CodeBuild.2 • Config.1 • DMS.1 • EC2.1 • EC2.2 • EC2.3 • EC2.4 • EC2.6 • EC2.7 • EC2.8 • EFS.1 • ELBV2.1 • EMR.1 • ES.1 • GuardDuty.1 • IAM.1

CIS Foundation Benchmark	PCI DSS	AWS Foundational Security Best Practices
<ul style="list-style-type: none"> • 2.5 • 2.6 • 2.7 • 2.8 • 2.9 • 3.1 • 3.2 • 3.3 • 3.4 • 3.5 • 3.6 • 3.7 • 3.8 • 3.9 • 3.10 • 3.11 • 3.12 • 3.13 • 3.14 • 4.1 • 4.2 • 4.3 	<ul style="list-style-type: none"> • PCI.IAM.2 • PCI.IAM.3 • PCI.IAM.4 • PCI.IAM.5 • PCI.IAM.6 • PCI.IAM.7 • PCI.IAM.8 • PCI.KMS.1 • PCI.Lambda.1 • PCI.Lambda.2 • PCI.RDS.1 • PCI.RDS.2 • PCI.Redshift.1 • PCI.S3.1 • PCI.S3.2 • PCI.S3.3 • PCI.S3.4 • PCI.S3.5 • PCI.S3.6 • PCI.SageMaker.1 • PCI.SSM.1 • PCI.SSM.2 • PCI.SSM.3 	<ul style="list-style-type: none"> • IAM.2 • IAM.3 • IAM.4 • IAM.5 • IAM.6 • IAM.7 • IAM.8 • KMS.1 • KMS.2 • Lambda.1 • Lambda.2 • RDS.1 • RDS.2 • RDS.3 • RDS.4 • RDS.5 • RDS.6 • RDS.7 • RDS.8 • S3.1 • S3.2 • S3.3 • S3.4 • S3.5 • S3.6 • SageMaker.1 • SecretsManager.1 • SecretsManager.2 • SSM.1 • SSM.2 • SSM.3

API calls supported by AWS Audit Manager

AWS 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 when you configure a control in Audit Manager.

For every resource that is in the scope of an API call, AWS 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 you run an `ec2_DescribeRouteTables` API call that captures configuration snapshots from five route tables, then you will get five pieces of evidence in total for the API call. Each piece of evidence is a snapshot of the configuration of an individual route table.

The following list of API calls are supported in Audit Manager.

Supported API calls to AWS services

- [iam_GenerateCredentialReport](#)
- [iam_GetAccountSummary](#)
- [iam_ListPolicies](#)
- [iam_GetAccountPasswordPolicy](#)
- [iam_ListUsers](#)
- [iam_ListRoles](#)
- [iam_ListGroups](#)
- [ec2_DescribeInstances](#)
- [ec2_DescribeFlowLogs](#)
- [ec2_DescribeVpcs](#)
- [ec2_DescribeSecurityGroups](#)
- [ec2_DescribeNetworkAcls](#)
- [ec2_DescribeRouteTables](#)
- [ec2_DescribeVpcEndpoints](#)
- [cloudtrail_DescribeTrails](#)
- [config_DescribeDeliveryChannels](#)
- [config_DescribeConfigRules](#)
- [kms_ListKeys](#)
- [cloudwatch_DescribeAlarms](#)
- [elasticfilesystem_DescribeFileSystems](#)

AWS CloudTrail event names supported by AWS Audit Manager

You can capture AWS CloudTrail events as evidence in AWS Audit Manager by specifying a CloudTrail event name when you configure a control.

The following CloudTrail events are not supported by AWS Audit Manager:

- [kms_GenerateDataKey](#)
- [kms_Decrypt](#)
- [sts_AssumeRole](#)

For more information about CloudTrail events, see [Viewing Events with CloudTrail Event History](#) in the *AWS CloudTrail User Guide*.

AWS Audit Manager settings

You can review and configure your AWS Audit Manager settings at any time.

To access settings

1. Open the AWS Audit Manager console at <https://console.aws.amazon.com/auditmanager/home>.
2. In the left navigation pane, choose **Settings**.
3. Review and update your settings as needed, and then choose **Save**.

The following settings are available:

- [Permissions](#) (p. 129)
- [Data encryption](#) (p. 129)
- [Default audit owners \(optional\)](#) (p. 130)
- [Assessment report destination \(optional\)](#) (p. 130)
- [Notifications \(optional\)](#) (p. 131)
- [Delegated administrator \(optional\)](#) (p. 131)
- [AWS Config \(optional\)](#) (p. 132)
- [Security Hub \(optional\)](#) (p. 133)
- [Disable AWS Audit Manager](#) (p. 133)

Permissions

AWS Audit Manager uses a service-linked role to connect to data sources on your behalf. For more details, see [Using service-linked roles for AWS Audit Manager](#) (p. 178).

To review the AWS Identity and Access Management (IAM) policies that Audit Manager uses, choose **View IAM service-linked role permission**.

For information about service-linked roles, see [Using service-linked roles](#) in the *IAM User Guide*.

Data encryption

AWS Audit Manager automatically creates a unique AWS managed *customer managed key*. By default, your data is encrypted with this KMS key. Alternatively, you can specify a symmetric customer managed key that you created as the default key for Audit Manager encryption. Using your own KMS key gives you more flexibility, including the ability to create, rotate, and disable keys. By default, your data is encrypted with a KMS key that AWS owns and manages on your behalf. You can choose a different KMS key if you want to customize your encryption settings.

You can review and change your encryption settings as follows.

- To use the default KMS key that's provided by AWS Audit Manager, clear **Customize encryption settings (advanced)**.

- To use a customer managed key, select **Customize encryption settings (advanced)**. You can then choose an existing KMS key, or create one.

Important

To generate assessment reports successfully, your customer managed key (if you provide one) must be in the same AWS Region as your assessment. For a list of AWS Audit Manager Regions, see [AWS Regions and Endpoints](#) in the *Amazon Web Services General Reference*.

Note

When 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. For instructions, see [Allowing users in other accounts to use a KMS key](#) in the *AWS Key Management Service Service Developer Guide*.

For more information about how to create keys, see [Creating keys](#) in the *AWS Key Management Service User Guide*.

Default audit owners (optional)

You can specify the default audit owners who have primary access your assessments in AWS Audit Manager. You can choose from the AWS accounts listed in the table, or use the search bar to look for other AWS accounts.

You can review and change your default audit owners as follows.

- To add a default audit owner, select the check box next to the account name under **Audit owner**.
- To remove a default audit owner, clear the check box next to the account name under **Audit owner**.

For more information about audit owners, see [AWS Audit Manager concepts and terminology \(p. 2\)](#).

Assessment report destination (optional)

You can choose an Amazon S3 bucket in which AWS Audit Manager stores the assessment reports from your assessments.

You can review and change where Audit Manager stores your assessment reports as follows.

- To use an existing S3 bucket, choose the S3 bucket name in the dropdown list.
- To create a new S3 bucket, choose **Create new bucket**.

Important

To generate assessment reports successfully, your S3 bucket must be in the same AWS Region as your assessment. For a list of AWS Audit Manager Regions, see [AWS Regions and Endpoints](#) in the *Amazon Web Services General Reference*.

For more information about how to create an S3 bucket, see [Creating a bucket](#) in the *Amazon S3 User Guide*.

Notifications (optional)

AWS Audit Manager can send notifications to the SNS topic that you specify in this setting. If you are subscribed to that SNS topic, you will receive notifications when you sign in to Audit Manager.

You can review and change where AWS Audit Manager sends notifications as follows.

- To use an existing Amazon SNS topic, select the topic name from the dropdown menu.
- To create a new Amazon SNS topic, choose **Create new topic**.

To learn more about the list of actions that invoke notifications in AWS Audit Manager, see [Notifications in AWS Audit Manager \(p. 134\)](#).

For information about how to create an Amazon SNS topic, see [Creating an Amazon SNS topic](#) in the *Amazon SNS User Guide*.

Delegated administrator (optional)

If you use AWS Organizations and want to enable multi-account support for AWS Audit Manager, you can designate a member account in your organization as the delegated administrator for Audit Manager.

Prerequisites

- If your account is not yet part of an organization and you want to enable multi-account support for Audit Manager, 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 AWS Security Hub settings \(p. 21\)](#) so that Audit Manager can collect Security Hub evidence from your member accounts.
- When you designate a delegated administrator, make sure that the delegated administrator account has access on the KMS key that you provided when setting up AWS Audit Manager. To review and change your encryption settings, see [Data encryption \(p. 129\)](#).

Issues to consider

- 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, you should use the same delegated administrator account across all Regions.

You can review and change your delegated administrator account settings as follows.

Add a delegated administrator

Warning

After you designate a delegated administrator in your Audit Manager settings, your management account can no longer create additional assessments in AWS Audit Manager, and

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

To add a delegated administrator

1. From the **Delegated administrator** section of the Audit Manager settings page, choose **Add delegated administrator**.
2. Under **Delegated administrator account ID**, enter the ID of the delegated administrator account.
3. Choose **Delegate**.

Change a delegated administrator

Warning

When you change the delegated administrator, you continue to have access to the evidence that you previously collected under that account. However, Audit Manager stops collecting and attaching evidence to that delegated administrator account moving forward.

To change the current delegated administrator

1. From the **Delegated administrator** section of the Audit Manager settings page, choose **Edit**.
2. Choose **Remove** to remove the current delegated administrator account.
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**.

Remove a delegated administrator

Warning

When you remove a delegated administrator from your Audit Manager settings, or when you deregister a delegated administrator from AWS Organizations, you continue to have access to the evidence that you previously collected under that account. However, Audit Manager stops collecting and attaching evidence to that delegated administrator account moving forward.

To remove the current delegated administrator

1. From the **Delegated administrator** section of the Audit Manager settings page, choose **Edit**.
2. Choose **Remove** to remove the current delegated administrator account.
3. In the pop-up window that appears, choose **Remove** to confirm.

AWS Config (optional)

You can allow AWS Audit Manager to collect log data from AWS Config. Audit Manager will then perform additional analysis, and annotate that data to generate evidence automatically for the AWS services that feed logs into AWS Config. We recommend that you enable AWS Config for an optimal experience in Audit Manager.

To enable AWS Config, choose **Enable on AWS Config** to go to the page for that service. For information on how to enable AWS Config, see [Setting up AWS Config](#) in the *AWS Config Developer Guide*.

Security Hub (optional)

You can allow AWS Audit Manager to import AWS Security Hub findings for supported compliance standards such as the CIS Foundations Benchmark and PCI. When AWS Security Hub is enabled, Audit Manager also analyzes user events gathered from CloudTrail, CloudWatch, and AWS Config, matches them to Security Hub findings, and uses them to generate audit evidence. We recommend that you enable AWS Security Hub for an optimal experience in Audit Manager.

To enable AWS Security Hub, choose **Enable Security Hub** to go to the page for that service. For information on how to enable AWS Security Hub, see [Setting up AWS Security Hub](#) in the *Security Hub User Guide*.

Disable AWS Audit Manager

You can disable AWS Audit Manager if you no longer want to use the service.

Warning

When you disable Audit Manager, your access is revoked and the service will no longer collect evidence for any existing assessments. You will not be able to access anything in the service unless you register again.

To disable Audit Manager, choose **Disable AWS Audit Manager**.

To re-enable AWS Audit Manager after you disable it, you must go to the 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. 18).

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 and its evidence for review. This notification is invoked when an audit owner chooses **Delegate control set** on the assessment summary page.
- A delegate completes their review of a control set. This notification is invoked when the delegate chooses **Submit for review** on the assessment summary page.

Prerequisites

Before you set up Amazon SNS notifications in AWS 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 (that is, a mobile phone number) to the topic. To receive notifications by email, subscribe an email endpoint (an email address) to the topic.

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 have to add permissions to the AWS KMS key policy. You can add permissions by attaching the following policy to the AWS KMS key policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAuditManagerToUseKMSKey",
      "Effect": "Allow",
      "Principal": {
        "Service": "auditmanager.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*"
    }
  ]
}
```

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**.

Note

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 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](#).

Troubleshooting

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 AWS KMS key. An example policy is available in the [Prerequisites \(p. 134\)](#) section of this page.
- 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 have to confirm your subscription before you start receiving email notifications. For more information, see [Getting Started](#) in the *Amazon SNS Developer Guide*.

Troubleshooting in AWS Audit Manager

You can use the following information to troubleshoot issues that you encounter when working with AWS Audit Manager.

Topic list

- [Troubleshooting evidence collection issues \(p. 136\)](#)
- [Troubleshooting permission and access issues \(p. 139\)](#)
- [Troubleshooting control and control set issues \(p. 141\)](#)
- [Troubleshooting assessment report issues \(p. 141\)](#)
- [Troubleshooting delegated administrator issues \(p. 143\)](#)
- [Troubleshooting notification issues \(p. 145\)](#)

Troubleshooting evidence collection issues

You can use the information on this page to resolve common evidence collection issues in Audit Manager.

Topics

- [I created an assessment but I can't see any evidence yet \(p. 136\)](#)
- [My assessment isn't collecting any evidence from AWS Security Hub \(p. 137\)](#)
- [My assessment isn't collecting evidence from another AWS service \(p. 138\)](#)
- [My evidence is generated at different intervals, and I don't understand how often it's being collected \(p. 138\)](#)

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 more than 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 are displaying results for these checks. The AWS Config and Security Hub results should be displaying in the same AWS Region that you use Audit Manager in.

If you still can't see any evidence in your assessment and it's not because of one of these issues, consider checking for the other issues that are described on this page.

My assessment isn't collecting any evidence from AWS Security Hub

This issue can be caused if you missed some configuration steps in your AWS Security Hub settings.

If you're using a single AWS account, you must enable AWS Config and the PCI DSS security standard for your account.

If you're using Organizations, you must do the following:

- Enable AWS Config and the PCI DSS security standard for every member account.
- Designate the same administrator account in Security Hub and in Audit Manager.

Make sure that you configured your Security Hub settings as follows.

Configuring Security Hub settings for a single AWS account

Before you enable any security standards in Security Hub, make sure that you enabled AWS Config and configured resource recording. For more information, see [Enabling and configuring AWS Config](#) in the *AWS Security Hub User Guide*. Then, follow this procedure to configure your Security Hub settings for Audit Manager.

To configure Security Hub settings for a single account

1. Sign in to the AWS Management Console and open the AWS Security Hub console at <https://console.aws.amazon.com/securityhub/>.
2. In the left navigation pane, choose **Security standards**.
3. Under **PCI DSS v3.2.1**, choose **Enable** to enable the PCI DSS security standard for your account. By default, the *AWS CIS Foundations Benchmark* standard and the *AWS Foundational Best Practices* standard are already enabled. For more information, see [Enabling a security standard](#) in the *AWS Security Hub User Guide*.

Configuring Security Hub settings for an organization

Before you enable any security standards in Security Hub, make sure that you enabled AWS Config and configured resource recording for your organization. For more information, see [Enabling and configuring AWS Config](#) in the *AWS Security Hub User Guide*. Then, follow this procedure to configure your Security Hub settings for Audit Manager.

To configure Security Hub settings for an organization

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. Make sure that the delegated administrator account that you designate in Security Hub is the same one that you designated in Audit Manager. For more information, see [Designating a Security Hub administrator account](#) in the *AWS Security Hub User Guide*.
3. Using your Organizations delegated administrator account, go to **Settings, Accounts** and enable your organization accounts as Security Hub member accounts. For more instructions, see [Enabling member accounts from your organization](#) in the *AWS Security Hub User Guide*.

4. Enable the *PCI DSS* security standard for every member account of the organization. By default, the *AWS CIS Foundations Benchmark* standard and the *AWS Foundational Best Practices* standard are already enabled. For more information, see [Enabling a security standard](#) in the *AWS Security Hub User Guide*.

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 don't understand how often it's being collected

The controls in Audit Manager assessments are mapped to a combination of 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 the resource state and change data without a compliance determination.

The following is a summary of the different data sources and their evidence collection frequency.

Data source	Description	Evidence collection frequency	When this control is active
AWS CloudTrail	Tracks a specified user activity that's needed in your audit.	Continual	Audit Manager assesses your CloudTrail logs and filters the relevant logs based on your keyword. The processed logs are converted into User activity evidence.
AWS Security Hub	Captures snapshots of your resource security posture in addition to the configuration changes that Security Hub checked.	Based on the schedule of the Security Hub check (typically around every 12 hours)	Audit Manager assesses the Security Hub findings that are associated with this Security Hub check. The processed data is converted into Compliance check evidence.

Data source	Description	Evidence collection frequency	When this control is active
AWS Config	Captures snapshots of your resource security posture in addition to the configuration changes that AWS Config evaluated.	Based on the settings defined in the AWS Config rule	Audit Manager assesses the CloudTrail logs that are associated with this AWS Config rule evaluation. The processed data is converted into Compliance check evidence.
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, and assesses the results. The results are converted into 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 about control data sources, see [Supported control data sources for automated evidence](#) and [Changing the evidence collection frequency for a control](#).

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 \(p. 139\)](#)
- [I specified someone as an audit owner, but they still don't have full access to the assessment. Why is this? \(p. 140\)](#)
- [I specified an Amazon SNS topic in Audit Manager, but I'm not receiving any notifications \(p. 145\)](#)
- [I can't perform an action in Audit Manager \(p. 140\)](#)
- [I'm an administrator and want to allow others to access Audit Manager \(p. 140\)](#)
- [I want to allow people outside of my AWS account to access my Audit Manager resources \(p. 140\)](#)

I followed the Audit Manager setup procedure, but I don't have enough IAM privileges

The IAM identity (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 for your IAM identities. 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 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 attach the appropriate permissions to the IAM identity. 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](#). For instructions on 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 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 user name and password.

I'm an administrator and want to allow others to access Audit Manager

To allow others to access AWS Audit Manager, you must create an IAM entity (user or role) for the person or application that needs access. They will use the credentials for that entity to access AWS. You must then attach a policy to the entity that grants them the correct permissions in AWS Audit Manager.

To get started right away, see [Creating your first IAM delegated user and group](#) in the *IAM User Guide*.

I want to allow people outside of my AWS account to access my Audit Manager resources

To grant people who are outside of your AWS account access to your Audit Manager resources, create an IAM role for them. You can do this both for users that are in other accounts and for people who are outside your organization. Using this role, they can access your resources. When you create the role, make sure that you specify who's trusted to assume the role.

To learn more, see the following topics in the *IAM User Guide*:

- For instructions on how to provide access to your resources across the AWS accounts that you own, see [Providing access to an IAM user in another AWS account that you own](#) in the *IAM User Guide*.
- For instructions on how to provide third-party AWS accounts with access to your resources, see [Providing access to AWS accounts owned by third parties](#) in the *IAM User Guide*.

- For instructions on how to provide access through identity federation, see [Providing access to externally authenticated users \(identity federation\)](#) in the *IAM User Guide*.

Troubleshooting control and control set issues

You can use the information on this page to resolve common issues with controls in Audit Manager.

Topics

- [I can't see any controls or control sets in my assessment \(p. 141\)](#)
- [I can't upload manual evidence to a control \(p. 141\)](#)

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.

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 \(p. 142\)](#)
- [I followed the checklist above, and my assessment report still failed to generate \(p. 142\)](#)
- [I'm unable to unzip the assessment report \(p. 142\)](#)
- [I get an *access denied* error when I try to generate a report \(p. 143\)](#)

- [My assessment report generation is stuck in *In progress* status, and I'm not sure how this impacts my billing \(p. 143\)](#)

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 S3 bucket match the AWS Region of your assessment?** The S3 bucket that you use as your assessment report destination must be in the same AWS Region as your assessment. For instructions on how to change the S3 bucket, see [AWS Audit Manager settings, Assessment report destination](#).
 - b. **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 [AWS Audit Manager settings, Data encryption](#).
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 configure the assessment report destination and the KMS key that's used for data encryption, see [AWS Audit Manager settings](#).

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 can support up to approximately 22,000 evidence items in a single assessment report. 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'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.

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.

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](#).

Troubleshooting delegated administrator 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 \(p. 144\)](#)
- [I get an *access denied* error when I try to generate an assessment report using my delegated administrator account \(p. 144\)](#)

- [When I create an assessment, I can't see the accounts from my organization under *Accounts in scope* \(p. 144\)](#)

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 11111111111 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.

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 \(p. 145\)](#)

I specified an Amazon SNS topic in Audit Manager, but I'm not receiving any notifications

You probably aren't receiving notification for one of two reasons. First, if your Amazon SNS topic uses AWS KMS for server-side encryption (SSE), you might be missing the required permissions for your KMS key policy. Second, 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*.

Quotas 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 cannot be increased. The following AWS Audit Manager quotas are per AWS account per Region.

Assessments

- Number of active assessments per account: 100

Controls

- Number of custom controls per account: 500

Frameworks

- Number of custom frameworks per account: 100

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. 147)
- [Identity and access management for AWS Audit Manager](#) (p. 149)
- [Compliance validation for AWS Audit Manager](#) (p. 180)
- [Resilience in AWS Audit Manager](#) (p. 180)
- [Infrastructure security in AWS Audit Manager](#) (p. 181)
- [AWS Audit Manager and interface VPC endpoints \(AWS PrivateLink\)](#) (p. 181)
- [Logging and monitoring in AWS Audit Manager](#) (p. 182)
- [Configuration and vulnerability analysis in AWS Audit Manager](#) (p. 185)

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 user accounts with 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 recommend TLS 1.2 or later.

- 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 personal 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 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 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 AWS Audit Manager customers do not include sensitive identifying information in the free-form **Delegation comment** and **Assessment report description** fields.

AWS Audit Manager retains customer data on a fast storage for up to one year. By default, your data will be deleted after one year.

Encryption at rest

To encrypt data at rest, AWS 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, AWS 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.

AWS 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 AWS 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 Amazon S3 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

AWS 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

AWS Audit Manager supports both AWS owned keys owned and customer managed keys for encrypting all Audit Manager resources (assessments, controls, frameworks, evidence, and assessment reports saved to Amazon 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, AWS 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 AWS 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 AWS Audit Manager using the AWS Management Console, API, or AWS Command Line Interface (AWS CLI). For more information, see [Step 4: Enable AWS Audit Manager \(p. 21\)](#).

You can review and change these settings at any time by choosing **Settings** in the left navigation pane of AWS Audit Manager.

- To use the AWS owned key provided by AWS Audit Manager, clear **Customize encryption settings (advanced)**.
- To use your own customer managed key, select **Customize encryption settings (advanced)**. You can then choose an existing KMS key, or create a new one.

For more information about how to change this setting, see [Data encryption \(p. 129\)](#).

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 AWS Audit Manager resources. IAM is an AWS service that you can use with no additional charge.

Topics

- [Audience \(p. 150\)](#)
- [Authenticating with identities \(p. 150\)](#)
- [Managing access using policies \(p. 152\)](#)
- [How AWS Audit Manager works with IAM \(p. 153\)](#)
- [Identity-based policy examples for AWS Audit Manager \(p. 159\)](#)
- [AWS managed policies for AWS Audit Manager \(p. 168\)](#)
- [Troubleshooting AWS Audit Manager identity and access \(p. 176\)](#)

- [Using service-linked roles for AWS Audit Manager \(p. 178\)](#)

Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work that you do in AWS Audit Manager.

Service user – If you use the AWS Audit Manager service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more AWS 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 AWS Audit Manager, see [Troubleshooting AWS Audit Manager identity and access \(p. 176\)](#).

Service administrator – If you're in charge of AWS Audit Manager resources at your company, you probably have full access to AWS Audit Manager. It's your job to determine which AWS Audit Manager features and resources your employees 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 AWS Audit Manager, see [How AWS Audit Manager works with IAM \(p. 153\)](#).

IAM administrator – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to AWS Audit Manager. To view example AWS Audit Manager identity-based policies that you can use in IAM, see [Identity-based policy examples for AWS Audit Manager \(p. 159\)](#).

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. For more information about signing in using the AWS Management Console, see [Signing in to the AWS Management Console as an IAM user or root user](#) in the *IAM User Guide*.

You must be *authenticated* (signed in to AWS) as the AWS account root user, an IAM user, or by assuming an IAM role. You can also use your company's single sign-on authentication or even sign in using Google or Facebook. In these cases, your administrator previously set up identity federation using IAM roles. When you access AWS using credentials from another company, you are assuming a role indirectly.

To sign in directly to the [AWS Management Console](#), use your password with your root user email address or your IAM user name. You can access AWS programmatically using your root user or IAM users access keys. AWS provides SDK and command line tools to cryptographically sign your request using your credentials. If you don't use AWS tools, you must sign the request yourself. Do this using *Signature Version 4*, a protocol for authenticating inbound API requests. For more information about authenticating requests, see [Signature Version 4 signing process](#) in the *AWS General Reference*.

Regardless of the authentication method that you use, you might also 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 [Using multi-factor authentication \(MFA\) in AWS](#) in the *IAM User Guide*.

AWS account root user

When you first create an AWS account, you begin with a single 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 do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the [best practice of using the root user only to create your first IAM user](#). Then securely lock away the root user credentials and use them to perform only a few account and service management tasks.

IAM users and groups

An *IAM user* is an identity within your AWS account that has specific permissions for a single person or application. An IAM user can have long-term credentials such as a user name and password or a set of access keys. To learn how to generate access keys, see [Managing access keys for IAM users](#) in the *IAM User Guide*. When you generate access keys for an IAM user, make sure you view and securely save the key pair. You cannot recover the secret access key in the future. Instead, you must generate a new access key pair.

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:

- **Temporary IAM user permissions** – An IAM user can assume an IAM role to temporarily take on different permissions for a specific task.
- **Federated user access** – Instead of creating an IAM user, you can use existing identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as *federated users*. AWS assigns a role to a federated user when access is requested through an [identity provider](#). For more information about federated users, see [Federated users and roles](#) in the *IAM User Guide*.
- **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 IAM 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 IAM identities or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. You can sign in as the root user or an IAM user, or you can assume an IAM role. When you then make a request, AWS evaluates the related identity-based or resource-based policies. 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**.

Every IAM entity (user or role) starts with no permissions. In other words, by default, users can do nothing, not even change their own password. To give a user permission to do something, an administrator must attach a permissions policy to a user. Or the administrator can add the user to a group that has the intended permissions. When an administrator gives permissions to a group, all users in that group are granted those permissions.

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 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 AWS Audit Manager, learn what IAM features are available to use with AWS Audit Manager.

IAM features you can use with AWS Audit Manager

IAM feature	Audit Manager support
Identity-based policies (p. 154)	Yes

IAM feature	Audit Manager support
Resource-based policies (p. 155)	No
Policy actions (p. 155)	Yes
Policy resources (p. 156)	Yes
Policy condition keys (p. 157)	Partial
ACLs (p. 158)	No
ABAC (tags in policies) (p. 158)	Yes
Temporary credentials (p. 158)	Yes
Principal permissions (p. 159)	Yes
Service roles (p. 159)	No
Service-linked roles (p. 159)	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: Example 3: Allow IAM users management access to AWS Audit Manager (p. 165). 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 AWS Audit Manager identity-based policies, see [Identity-based policy examples for AWS Audit Manager \(p. 159\)](#).

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 AWS Audit Manager identity-based policies, see [Identity-based policy examples for AWS Audit Manager](#) (p. 159).

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:${Partition}:audit-manager:${Region}:${Account}:assessment/${assessmentId}
```

An Audit Manager control set has the following ARN format:

```
arn:${Partition}:audit-manager:${Region}:${Account}:assessment/${assessmentId}controlSet/${controlSetId}
```

An Audit Manager control has the following ARN format:

```
arn:${Partition}:audit-manager:${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:audit-manager:us-east-1:123456789012:assessment/i-1234567890abcdef0"
```

To specify all instances that belong to a specific account, use the wildcard (*).

```
"Resource": "arn:aws:audit-manager:us-east-1:123456789012:assessment/*"
```

Some AWS 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 accessible by the currently logged in AWS account. So an IAM 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 AWS 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 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.

You can also use placeholder variables when you specify conditions. For example, you can grant an IAM user permission to access a resource only if it is tagged with their IAM user name. For more information, see [IAM policy elements: variables and tags](#) in the *IAM User Guide*.

AWS 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.

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. 186).

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 IAM 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. 178).

Identity-based policy examples for AWS Audit Manager

By default, IAM users and roles don't have permission to create or modify AWS Audit Manager resources. They also can't perform tasks using the AWS Management Console, AWS CLI, or AWS API. An IAM administrator must create IAM policies that grant users and roles permission to perform actions on the resources that they need. The administrator must then attach those policies to the IAM users or groups that require those permissions.

To learn how to create an IAM identity-based policy using these example JSON policy documents, see [Creating policies on the JSON tab](#) in the *IAM User Guide*.

Topics

- [Policy best practices](#) (p. 160)
- [Example 1: Minimum permissions required to enable AWS Audit Manager](#) (p. 160)
- [Example 2: Allow IAM users full administrator access to AWS Audit Manager](#) (p. 161)
- [Example 3: Allow IAM users management access to AWS Audit Manager](#) (p. 165)
- [Example 4: Allow IAM users read-only access to AWS Audit Manager](#) (p. 166)
- [Example 5: Allow users to view their own permissions](#) (p. 167)
- [Example 6: Allow AWS Audit Manager to send notifications to Amazon SNS topics](#) (p. 167)

Policy best practices

Identity-based policies are very powerful. They determine whether someone can create, access, or delete AWS 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 using AWS managed policies** – To start using AWS Audit Manager quickly, use AWS managed policies to give your employees the permissions they need. These policies are already available in your account and are maintained and updated by AWS. For more information, see [Get started using permissions with AWS managed policies](#) in the *IAM User Guide*.
- **Grant least privilege** – When you create custom policies, grant only the permissions required to perform a task. Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later. For more information, see [Grant least privilege](#) in the *IAM User Guide*.
- **Enable MFA for sensitive operations** – For extra security, require IAM users to use multi-factor authentication (MFA) to access sensitive resources or API operations. For more information, see [Using multi-factor authentication \(MFA\) in AWS](#) in the *IAM User Guide*.
- **Use policy conditions for extra security** – To the extent that it's practical, define the conditions under which your identity-based policies allow access to a resource. For example, you can write conditions to specify a range of allowable IP addresses that a request must come from. You can also write conditions to allow requests only within a specified date or time range, or to require the use of SSL or MFA. For more information, see [IAM JSON policy elements: Condition](#) in the *IAM User Guide*.

Example 1: Minimum permissions required to enable AWS Audit Manager

This example shows how you might allow accounts without an administrator role to enable AWS Audit Manager. This is a basic policy that grants the minimum permissions needed to enable Audit Manager.

To grant the minimum permissions required to use Audit Manager, attach the following policy to an IAM identity. 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*.

```
{
  "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": {
            "StringEquals": {
                "events:source": "aws.securityhub",
                "events:detail-type": "Security Hub Findings - Imported"
            }
        }
    },
    {
        "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.

Example 2: Allow IAM users full administrator access to AWS Audit Manager

The policies in this example grant full administrator access to AWS Audit Manager. This includes the ability to enable and disable Audit Manager, the ability to change settings in Audit Manager, and the ability to manage all Audit Manager resources such as assessments, frameworks, controls, and assessment reports.

The first policy in this example is the managed policy, `AWSAuditManagerAdministratorAccess`. The second policy in this example provides permissions for the Amazon S3 bucket that you use as an assessment report destination in AWS Audit Manager.

Policy 1 (Managed policy, `AWSAuditManagerAdministratorAccess`)

```
{
  "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:EnableAWSServiceAccess"
      ],
      "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:source": "aws.securityhub",
          "events:detail-type": "Security Hub Findings - Imported"
        }
      }
    }
  ]
}

```

```
    }
  },
  {
    "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": "*"
  }
]
```

Policy 2 (Assessment report destination permissions)

Replace the *placeholders* with your own information. You should include the S3 bucket that you specified when you created an assessment report destination in AWS Audit Manager, and the key used 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::assessment-reports-destination/*"
    }
  ],
  {
    "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: Allow IAM 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": "SNSAccess",
    "Effect": "Allow",
    "Action": [
      "sns:ListTopics"
    ],
    "Resource": "*"
  },
  {
    "Sid": "TagAccess",
    "Effect": "Allow",
    "Action": [
      "tag:GetResources"
    ],
    "Resource": "*"
  }
]
```

Example 4: Allow IAM 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": "*"
    }
  ]
}
```

Example 5: 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": "*"
    }
  ]
}
```

Example 6: Allow AWS Audit Manager to send notifications to Amazon SNS topics

This policy grants AWS Audit Manager permissions to send notifications to an existing Amazon SNS topic. If you want to receive notifications from Audit Manager, attach the following permissions to the access policy of your Amazon SNS topic. You must substitute appropriate values for *region*, *account-id*, and *myTopic*.

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "auditmanager.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic"
    }
  ]
}
```

AWS managed policies for AWS Audit Manager

To add permissions to users, groups, and roles, it is easier to use AWS managed policies than to write policies yourself. It takes time and expertise to [create IAM customer managed policies](#) that provide your team with only the permissions they need. To get started quickly, you can use our AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see [AWS managed policies](#) in the *IAM User Guide*.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the **ViewOnlyAccess** AWS managed policy provides read-only access to many AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see [AWS managed policies for job functions](#) in the *IAM User Guide*.

Topics

- [AWS managed policy: AWSAuditManagerAdministratorAccess](#) (p. 168)
- [AWS managed policy: AWSAuditManagerServiceRolePolicy](#) (p. 171)
- [AWS Audit Manager updates to AWS managed policies](#) (p. 176)

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:EnableAWSServiceAccess"
      ],
      "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:source": "aws.securityhub",
            "events:detail-type": "Security Hub Findings - Imported"
        }
    }
},
{
    "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 do the following on your behalf:

- Collect and assess data from the following data sources to generate AWS Audit Manager evidence:
 - Management events from AWS CloudTrail
 - Compliance checks from AWS Config Rules
 - Compliance checks from AWS Security Hub
- Describe APIs specific to the following services:
 - AWS CloudTrail

- Amazon CloudWatch
- Amazon Cognito user pools
- AWS Config
- Amazon EC2
- Amazon EFS
- Amazon EventBridge
- Amazon GuardDuty
- AWS Identity and Access Management (IAM)
- AWS KMS
- AWS License Manager
- AWS Organizations
- Amazon Route 53
- Amazon S3
- AWS Security Hub
- AWS WAF

Permissions details

`AWSAuditManagerServiceRolePolicy` allows AWS Audit Manager to complete the following actions on the specified resources:

- `license-manager:ListAssociationsForLicenseConfiguration`
- `license-manager:ListUsageForLicenseConfiguration`
- `iam:GenerateCredentialReport`
- `iam:GetAccountSummary`
- `iam:ListPolicies`
- `iam:GetAccountPasswordPolicy`
- `iam:ListUsers`
- `iam:ListUserPolicies`
- `iam:ListRoles`
- `iam:ListRolePolicies`
- `iam:ListGroups`
- `iam:ListGroupPolicies`
- `iam:ListEntitiesForPolicy`
- `ec2:DescribeInstances`
- `ec2:DescribeFlowLogs`
- `ec2:DescribeVpcs`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSnapshots`
- `ec2:DescribeVpcEndpoints`
- `cloudtrail:DescribeTrails`
- `config:DescribeDeliveryChannels`
- `config:ListDiscoveredResources`
- `config:DescribeConfigRules`

- kms:ListKeys
- kms:DescribeKey
- kms:ListGrants
- cloudwatch:DescribeAlarms
- s3:GetLifecycleConfiguration
- events:DescribeRule
- route53:GetQueryLoggingConfig
- organizations:DescribePolicy
- cognito-idp:DescribeUserPool
- elasticfilesystem:DescribeFileSystems

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "license-manager:ListLicenseConfigurations",
        "license-manager:ListAssociationsForLicenseConfiguration",
        "license-manager:ListUsageForLicenseConfiguration"
      ],
      "Resource": "*",
      "Sid": "LicenseManagerAccess"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GenerateCredentialReport",
        "iam:GetAccountSummary",
        "iam:ListPolicies",
        "iam:GetAccountPasswordPolicy",
        "iam:ListUsers",
        "iam:ListUserPolicies",
        "iam:ListRoles",
        "iam:ListRolePolicies",
        "iam:ListGroups",
        "iam:ListGroupPolicies",
        "iam:ListEntitiesForPolicy"
      ],
      "Resource": "*",
      "Sid": "IAMAccess"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource": "*",
      "Sid": "EC2Access"
    },
    {
      "Effect": "Allow",
      "Action": [
```

```

        "cloudtrail:DescribeTrails"
    ],
    "Resource": "*",
    "Sid": "CloudtrailAccess"
},
{
    "Effect": "Allow",
    "Action": [
        "config:DescribeDeliveryChannels",
        "config:ListDiscoveredResources",
        "config:DescribeConfigRules"
    ],
    "Resource": "*",
    "Sid": "ConfigAccess"
},
{
    "Effect": "Allow",
    "Action": [
        "securityhub:DescribeStandards"
    ],
    "Resource": "*",
    "Sid": "SecurityHubAccess"
},
{
    "Effect": "Allow",
    "Action": [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:ListGrants"
    ],
    "Resource": "*",
    "Sid": "KMSAccess"
},
{
    "Effect": "Allow",
    "Action": [
        "cloudwatch:DescribeAlarms"
    ],
    "Resource": "*",
    "Sid": "CloudwatchAccess"
},
{
    "Effect": "Allow",
    "Action": [
        "s3:GetLifecycleConfiguration"
    ],
    "Resource": "*",
    "Sid": "S3Access"
},
{
    "Effect": "Allow",
    "Action": [
        "events:DescribeRule"
    ],
    "Resource": "*",
    "Sid": "EventBridgeAccess"
},
{
    "Effect": "Allow",
    "Action": [
        "waf:ListActivatedRulesInRuleGroup"
    ],
    "Resource": "*",
    "Sid": "WAFAccess"
},
{

```

```

        "Effect": "Allow",
        "Action": [
            "guarddduty:ListDetectors"
        ],
        "Resource": "*",
        "Sid": "GuardDutyAccess"
    },
    {
        "Effect": "Allow",
        "Action": [
            "route53:GetQueryLoggingConfig"
        ],
        "Resource": "*",
        "Sid": "Route53Access"
    },
    {
        "Effect": "Allow",
        "Action": [
            "organizations:DescribePolicy"
        ],
        "Resource": "*",
        "Sid": "OrganizationsAccess"
    },
    {
        "Effect": "Allow",
        "Action": [
            "cognito-idp:DescribeUserPool"
        ],
        "Resource": "*",
        "Sid": "CognitoAccess"
    },
    {
        "Effect": "Allow",
        "Action": [
            "elasticfilesystem:DescribeFileSystems"
        ],
        "Resource": "*",
        "Sid": "EFSAccess"
    },
    {
        "Sid": "CreateEventsAccess",
        "Effect": "Allow",
        "Action": [
            "events:PutRule"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "events:source": "aws.securityhub",
                "events:detail-type": "Security Hub Findings - Imported"
            }
        }
    },
    {
        "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
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 AWS Audit Manager and IAM.

Topics

- [I am not authorized to perform an action in AWS Audit Manager \(p. 176\)](#)
- [I am not authorized to perform iam:PassRole \(p. 176\)](#)
- [I want to view my access keys \(p. 177\)](#)
- [I'm an administrator and want to allow others to access AWS Audit Manager \(p. 177\)](#)
- [I want to allow people outside of my AWS account to access my AWS Audit Manager resources \(p. 177\)](#)

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, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password. Ask that person to update your policies to allow you to pass a role to AWS 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 AWS Audit Manager. However, the action requires the service to have permissions 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 asks her administrator to update her policies to allow her to perform the `iam:PassRole` action.

I want to view my access keys

After you create your IAM user access keys, you can view your access key ID at any time. However, you can't view your secret access key again. If you lose your secret key, you must create a new access key pair.

Access keys consist of two parts: an access key ID (for example, `AKIAIOSFODNN7EXAMPLE`) and a secret access key (for example, `wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY`). Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. Manage your access keys as securely as you do your user name and password.

Important

Do not provide your access keys to a third party, even to help [find your canonical user ID](#). By doing this, you might give someone permanent access to your account.

When you create an access key pair, you are prompted to save the access key ID and secret access key in a secure location. The secret access key is available only at the time you create it. If you lose your secret access key, you must add new access keys to your IAM user. You can have a maximum of two access keys. If you already have two, you must delete one key pair before creating a new one. To view instructions, see [Managing access keys](#) in the *IAM User Guide*.

I'm an administrator and want to allow others to access AWS Audit Manager

To allow others to access AWS Audit Manager, you must create an IAM entity (user or role) for the person or application that needs access. They will use the credentials for that entity to access AWS. You must then attach a policy to the entity that grants them the correct permissions in AWS Audit Manager.

To get started right away, see [Creating your first IAM delegated user and group](#) in the *IAM User Guide*.

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 AWS Audit Manager supports these features, see [How AWS Audit Manager works with IAM](#) (p. 153).
- 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 complete the following actions on the specified resources:

- `license-manager:ListAssociationsForLicenseConfiguration`
- `license-manager:ListUsageForLicenseConfiguration`
- `iam:GenerateCredentialReport`
- `iam:GetAccountSummary`
- `iam:ListPolicies`
- `iam:GetAccountPasswordPolicy`
- `iam:ListUsers`
- `iam:ListUserPolicies`
- `iam:ListRoles`
- `iam:ListRolePolicies`
- `iam:ListGroups`
- `iam:ListGroupPolicies`
- `iam:ListEntitiesForPolicy`
- `ec2:DescribeInstances`
- `ec2:DescribeFlowLogs`
- `ec2:DescribeVpcs`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSnapshots`
- `ec2:DescribeVpcEndpoints`
- `cloudtrail:DescribeTrails`

- `config:DescribeDeliveryChannels`
- `config:ListDiscoveredResources`
- `config:DescribeConfigRules`
- `kms:ListKeys`
- `kms:DescribeKey`
- `kms:ListGrants`
- `cloudwatch:DescribeAlarms`
- `s3:GetLifecycleConfiguration`
- `events:DescribeRule`
- `route53:GetQueryLoggingConfig`
- `organizations:DescribePolicy`
- `cognito-idp:DescribeUserPool`
- `elasticfilesystem:DescribeFileSystems`

To view the full permissions details of the service-linked role `AWSServiceRoleForAuditManager`, go to the Audit Manager console, choose **Settings**, and then choose **View IAM service-linked role permissions**.

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 a service-linked role for AWS Audit Manager

You don't need to manually create a service-linked role. When you enable AWS Audit Manager, the service automatically creates the service-linked role for you. You can enable Audit Manager from the onboarding page of the AWS Management Console, or via the API or AWS CLI. For more information, see [Step 4: Enable AWS Audit Manager \(p. 21\)](#) 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 a service-linked role for AWS Audit Manager

AWS Audit Manager does not allow you to edit the `AWSServiceRoleForAuditManager` service-linked role. After you create a service-linked role, you cannot 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"}}
```

}

Supported Regions for AWS Audit Manager service-linked roles

AWS Audit Manager supports using service-linked roles in all of the Regions where the service is available. For more information, see [AWS service endpoints](#).

Compliance validation for AWS Audit Manager

Third-party auditors assess the security and compliance of AWS services as part of multiple AWS compliance programs, such as SOC, PCI, FedRAMP, and HIPAA.

To learn whether Audit Manager or other AWS services are in scope of specific compliance programs, see [AWS Services in Scope by Compliance Program](#). 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 Whitepaper](#) – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.

Note

Not all services are compliant with HIPAA.

- [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 that helps you check your compliance with security industry standards and best practices.
- [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 the AWS global network security procedures that are described in the [Amazon Web Services: Overview of Security Processes](#) whitepaper.

You use AWS published API calls to access AWS Audit Manager through the network. Clients must support Transport Layer Security (TLS) 1.0 or later. We recommend TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). 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 [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 AWS 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](#).

Logging AWS Audit Manager API calls with AWS CloudTrail

AWS Audit Manager is integrated with AWS 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 AWS 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 AWS 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](#).

AWS Audit Manager information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in AWS 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 AWS 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 AWS 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 or AWS Identity and Access Management (IAM) 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 AWS 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 AWS Audit Manager resources. You can use tags as search criteria when browsing the Framework Library and 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 AWS Audit Manager

The following resources in AWS Audit Manager 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 and the Audit Manager API. For more information, see the following links.

- For assessments:
 - [Creating an assessment \(p. 33\)](#) and [Editing an assessment \(p. 37\)](#) in the *Assessments* section of this guide
 - [Tags tab \(p. 42\)](#) 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 \(p. 71\)](#) and [Editing a custom framework \(p. 74\)](#) in the *Framework library* section of this guide
 - [Tags tab \(p. 71\)](#) 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 \(p. 111\)](#) and [Editing a custom control \(p. 117\)](#) in the *Control library* section of this guide
 - [Tags tab \(p. 111\)](#) 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](#)

Using AWS Audit Manager with the AWS SDKs

This section contains links to the language-specific SDKs that you can use with Audit Manager. For more information, review the following topics.

Topics

- [AWS SDK for .NET \(p. 189\)](#)
- [AWS SDK for C++ \(p. 189\)](#)
- [AWS SDK for Go \(p. 189\)](#)
- [AWS SDK for Java 2.x \(p. 190\)](#)
- [AWS SDK for JavaScript \(p. 190\)](#)
- [AWS SDK for PHP V3 \(p. 190\)](#)
- [AWS SDK for Python \(Boto\) \(p. 190\)](#)
- [AWS SDK for Ruby V3 \(p. 190\)](#)

AWS SDK for .NET

You can use the AWS SDK for .NET to call AWS services using idiomatic .NET APIs. For more information, see the [AWS SDK for .NET](#). Choose **Get started with AWS SDK for .NET** on this page for step-by-step instructions to get started.

To see descriptions of the classes that are included in the AWS Audit Manager SDK for .NET, see the [AWS Audit Manager SDK for .NET](#).

AWS SDK for C++

The AWS SDK for C++ is a modern, open-source C++ library that makes it easy to integrate your C++ applications with AWS services. For more information, see the [AWS SDK for C++](#). Choose **Getting started** on this page for step-by-step instructions to get started.

To see descriptions of the classes that are included in the AWS Audit Manager SDK for C++, see the [AWS Audit Manager SDK for C++](#).

AWS SDK for Go

The AWS SDK for Go helps you integrate your Go applications with the full suite of AWS services. For more information, see the [AWS SDK for Go](#). Choose **Get started** on this page for step-by-step instructions to get started.

To see descriptions of the API client, operations, and parameter types for AWS Audit Manager, see the [AWS Audit Manager package in the AWS SDK for Go](#).

AWS SDK for Java 2.x

You can use the AWS SDK for Java to call AWS services using idiomatic Java APIs. For more information, see the [AWS SDK for Java](#). Choose **Get started with AWS SDK for Java** on this page for step-by-step instructions to get started.

To see descriptions of the AWS Audit Manager API operations for the AWS SDK for Java in detail, see the [AWS Audit Manager SDK for Java](#).

AWS SDK for JavaScript

The AWS SDK for JavaScript provides first class TypeScript support and enables you to call AWS services using idiomatic JavaScript APIs. For more information, see the [AWS SDK for JavaScript](#) for step-by-step instructions to get started.

To see descriptions of the AWS Audit Manager API operations for the AWS SDK for JavaScript in detail, see the [AWS Audit Manager SDK for JavaScript API](#).

AWS SDK for PHP V3

The AWS SDK for PHP is a modern, open-source PHP library that you can use to integrate your PHP applications with AWS services such as AWS Audit Manager. For more information, see the [AWS SDK for PHP](#). Choose **Getting started** on this page for step-by-step instructions to get started.

To see descriptions of the classes that are included in the AWS Audit Manager for PHP, see the [AWS Audit Manager SDK for PHP](#).

AWS SDK for Python (Boto)

Boto is a Python package that provides interfaces to AWS, including AWS Audit Manager. For more information about Boto, see the [AWS SDK for Python \(Boto\)](#). Choose **Getting started** on this page for step-by-step instructions to get started.

To see descriptions of the classes that are included in the AWS Audit Manager SDK for Python, see the [AWS Audit Manager SDK for Python \(Boto3\)](#).

Note

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

AWS SDK for Ruby V3

The AWS SDK for Ruby provides Ruby classes for many AWS services, including AWS Audit Manager. The SDK is provided for each AWS service as individual downloadable packages that include code and documentation. The SDK is also available through [Ruby Gems](#). For more information, see the [AWS SDK for Ruby](#) for step-by-step instructions to get started.

To see descriptions of the classes that are included in the AWS Audit Manager SDK for Ruby, see the [AWS Audit Manager SDK for Ruby](#).

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.

update-history-change	update-history-description	update-history-date
New examples of AWS Audit Manager controls (p. 191)	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
New supported framework: Gramm-Leach-Bliley Act (GLBA) (p. 191)	A new prebuilt framework is now available in AWS Audit Manager. For more information, see Gramm-Leach-Bliley Act (GLBA) .	September 2, 2021
New troubleshooting chapter (p. 191)	A new troubleshooting chapter is now available. For more information, see Troubleshooting in AWS Audit Manager .	August 23, 2021
New delegation chapter and tutorial (p. 191)	We expanded our delegation documentation into a new chapter. For more information, see Delegations in AWS Audit Manager . 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 Tutorial for Delegates: Reviewing a control set .	June 25, 2021
New supported framework: NIST SP 800-171 Rev. 2 (p. 191)	A new prebuilt framework is now available in AWS Audit Manager. For more information, see NIST SP 800-171 Rev. 2 .	June 17, 2021
Improved assessment reports (p. 191)	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 Assessment reports .	June 8, 2021

New AWS managed policies page (p. 191)	AWS Audit Manager has started tracking changes for its managed policies. For more information, see AWS managed policies for AWS Audit Manager .	May 6, 2021
New supported framework: NIST Cybersecurity Framework version 1.1 (p. 191)	A new prebuilt framework is now available in AWS Audit Manager. For more information, see NIST Cybersecurity Framework version 1.1 .	May 5, 2021
New supported framework: AWS Well-Architected (p. 191)	A new prebuilt framework is now available in AWS Audit Manager. For more information, see AWS Well-Architected .	May 5, 2021
New supported framework: AWS Foundational Security Best Practices (p. 191)	A new prebuilt framework is now available in AWS Audit Manager. For more information, see AWS Foundational Security Best Practices .	May 5, 2021
New supported framework: GxP EU Annex 11 (p. 191)	A new prebuilt framework is now available in AWS Audit Manager. For more information, see GxP EU Annex 11 .	April 28, 2021
New supported framework: NIST 800-53 (Rev. 5) Low-Moderate-High (p. 191)	A new prebuilt framework is now available in AWS Audit Manager. For more information, see NIST 800-53 (Rev. 5) Low-Moderate-High .	March 25, 2021
New supported frameworks: CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3 (p. 191)	Two new prebuilt frameworks are now available in AWS Audit Manager: <i>CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0, Level 1</i> , and <i>CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0, Level 1 and 2</i> . For more information, see CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.3.0 .	March 22, 2021
Initial release (p. 191)	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 General Reference*.