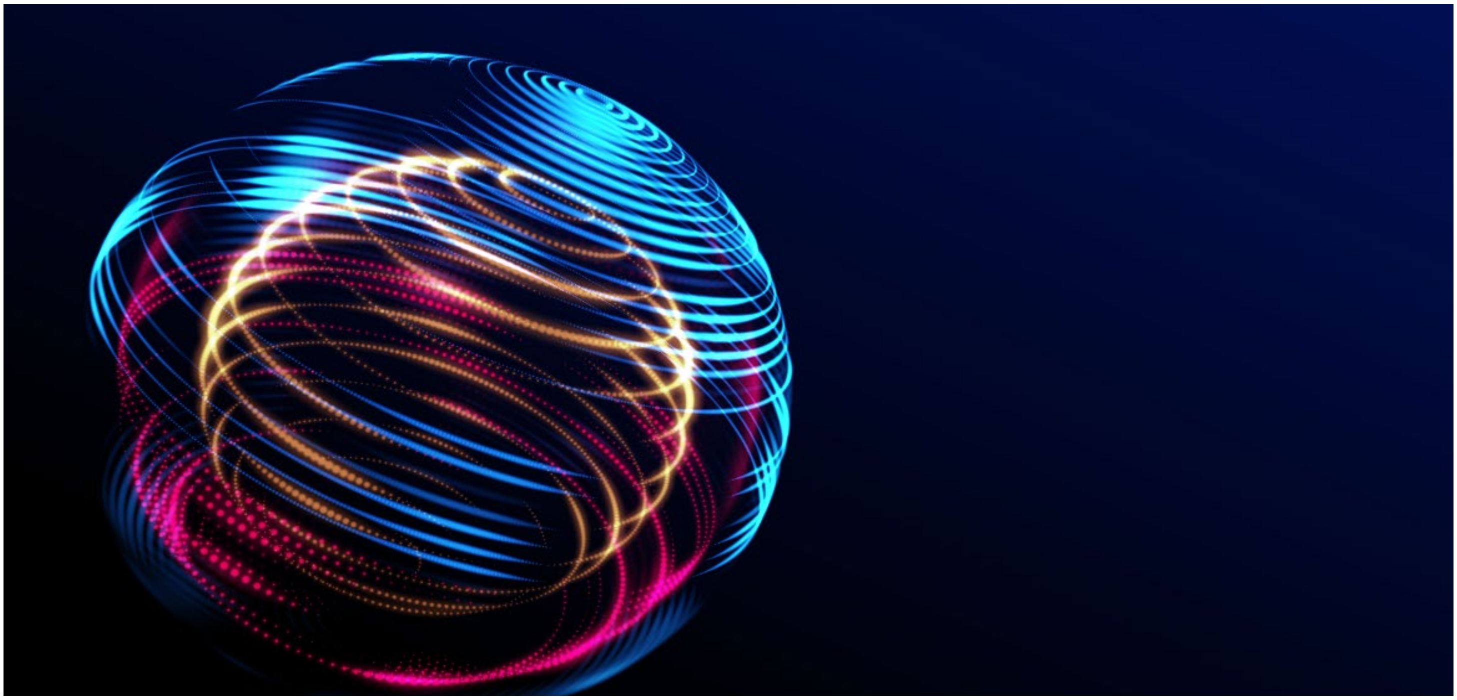
March 2021



Effective compliance and audit management using Amazon Web Services (AWS) Audit Manager

Managing risk and compliance

Organizations, especially those in highly regulated industries such as financial services and health care are subject to and undergo frequent audits as a result from various industry standards, legal and regulatory requirements (such as Payment Card Industry Data Security Standard (PCI-DSS), System and Organization Controls (SOC) and Health Insurance Portability Accountability Act (HIPAA)). Large and audit-mature organizations typically have well-established second and third lines to help identify control gaps and address risks. External auditors and regulators look at a variety of areas with the organization, so it is important to establish a controls-minded culture. As the enterprise cloud footprint increases, the focus of compliance and audit programs has also shifted to assets in the cloud.

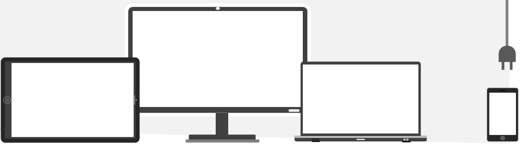
Managing compliance in AWS
The AWS Compliance Program helps customers to understand the broad controls in place at AWS to maintain security and compliance in the cloud. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS services (such as Config, Security Hub and CloudTrail) build on traditional programs, helping customers establish and operate in an AWS security control environment.

While AWS manages some of the compliance requirements in accordance with the shared responsibility model, AWS customers remain responsible for complying with applicable requirements for controls that they manage. A compliance assessment, therefore, includes a combination of controls managed by AWS and those that are managed by AWS customers.

Cyber risk and compliance processes within the cloud are as important as on-premises

When transitioning or implementing workloads into the cloud, one of the primary concerns of an organization is to manage risks and regulations and effectively demonstrate compliance. Not complying with regulatory requirements, or not having a strategy to effectively manage cloud and cyber risks, can lead to negative implications on businesses and the way they operate. A good cyber governance, risk, and compliance (GRC) program is fundamental to help secure the “crown jewels” (business critical assets) of an organization as it provides a broad approach to manage cyber risks and enable organizations to proactively meet their security and compliance objectives. As organizations look toward increasing adoption of cloud, they should also consider extending the cyber GRC program to address cloud services and gain greater visibility into exposure to related cyber risks.

AWS provides a suite of services that can be leveraged for securing workloads and automating compliance activities on AWS. By selecting and appropriately configuring a combination of AWS services that are relevant to the business, security teams can efficiently deploy security controls for people, processes, and technology to effectively demonstrate compliance with regulatory and governance requirements.



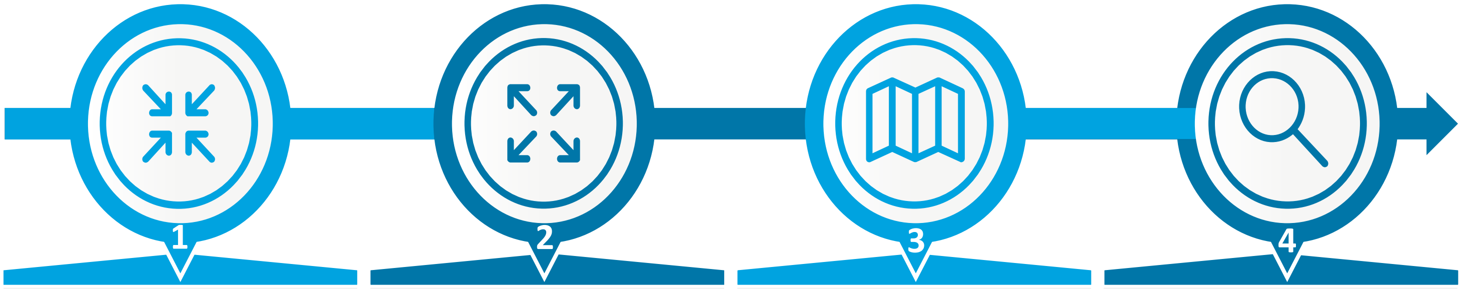
The downsides: Time spent pulling documentation, wasted resources, audit fatigue

In today’s regulatory climate, an organization’s second and third lines spend considerable time pulling evidences and artifacts to support annual audit and compliance requirements. Coordinating efforts between the second line, internal auditors, the external auditor, and financial regulators easily lend itself to audit fatigue. Efforts to capture, inventory, and manage evidence for ongoing audits and assessments across the enterprise is typically high, which can result in higher audit and compliance costs.

Streamlining audit management and compliance assessments through AWS Audit Manager

AWS Audit Manager helps you continuously evaluate your AWS usage to simplify how you assess risk and compliance with regulations and industry standards.

It allows the AWS customers to continuously gather, track, and organize evidence to support the execution of assessments/audits over their use of AWS services. Audit and GRC teams can collaborate in Audit Manager to review, curate, and finalize the evidence they want to publish as auditor-friendly artifacts. These artifacts are encrypted, durably stored, and can be cryptographically verified to avoid evidence tampering.



Comprehensive collection of logs

To monitor modifications and changes to an organization’s infrastructure, they collect logs from different sources. By allowing collection of logs from diverse log sources such as AWS CloudTrail, AWS Config, AWS Security Hub and AWS License Manager, Audit Manager provides broad evidence collection and simplifies the log management process.

Relevant evidence for specific audit scopes are automatically collected for review and validation, reducing “all hands on deck” effort required for both scheduled and short notice audits by continuously collecting evidence.

Universal log format

One major challenge while collecting log files from diverse sources is the varied formats that they come in. To read and analyze them, different applications might be required.

To help mitigate this issue, the tool translates the evidence into a consistent auditor-friendly format. This not only helps in streamlining the log analysis process but also reduces the risk of evidence tampering by using cryptographic verification so customers can archive and share artifacts with confidence.

Mapping evidence to the right audit controls

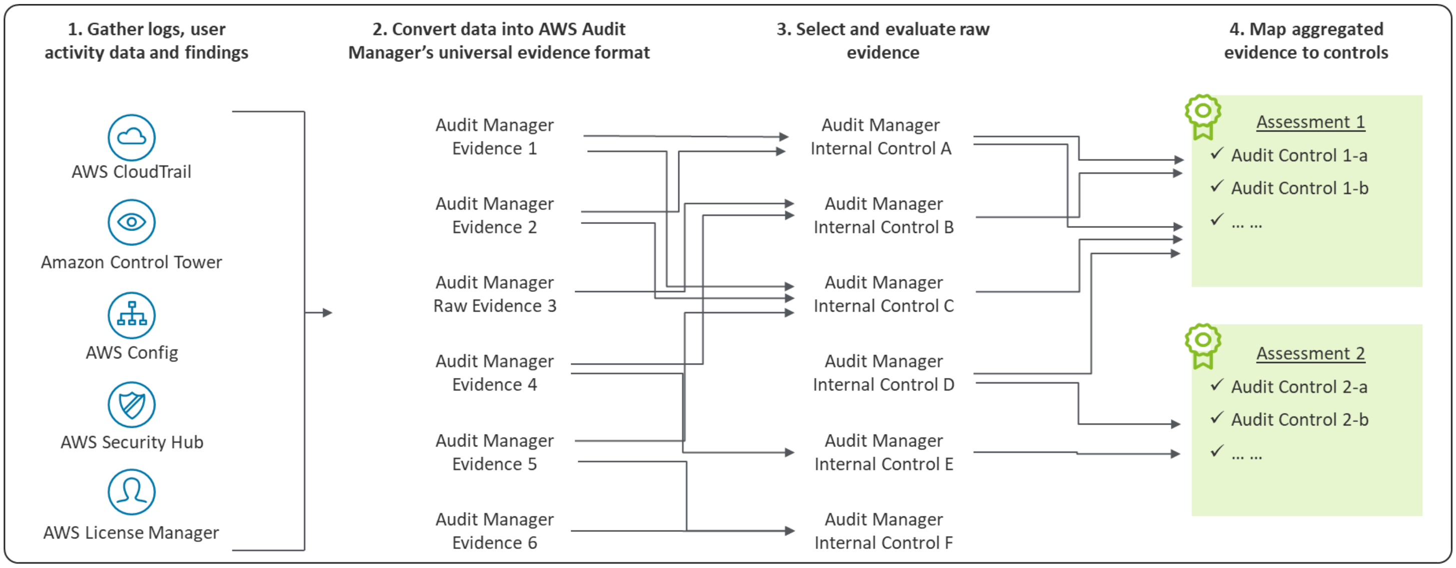
As the tool offers a curated gallery of pre-defined frameworks covering industry standards and legal / regulatory requirements (e.g., HIPAA, SOC2, PCI-DSS) and an easy way to define custom controls and frameworks needed to meet in-house audit requirements. The next step is to understand the requirements set by the user and automatically map the collected evidence to the accurate audit control.

Audit Manager uses the mappings within an assessment to suggest relevant evidence already saved from past audits and continuously collect new evidence from AWS services for audit teams to review.

Reviewing controls with evidence

As a next step, users can review each control in an assessment with the relevant evidence attached by Audit Manager. Audit Manager enables teamwork collaboration such as commenting and delegating control review to different users. This process distributes the efforts required in the control review to multiple internal teams.

Once finalized, Audit Manager uses the evidence in the assessment to produce immutable reports with integrity check to help prevent tampering.


1. Gather logs, user activity data and findings
2. Convert data into AWS Audit Manager's universal evidence format
3. Select and evaluate raw evidence
4. Map aggregated evidence to controls
AWS CloudTrail
Amazon Control Tower
AWS Config
AWS Security Hub
AWS License Manager
Audit Manager Evidence 1
Audit Manager Evidence 2
Audit Manager Raw Evidence 3
Audit Manager Evidence 4
Audit Manager Evidence 5
Audit Manager Evidence 6
Audit Manager Internal Control A
Audit Manager Internal Control B
Audit Manager Internal Control C
Audit Manager Internal Control D
Audit Manager Internal Control E
Audit Manager Internal Control F
Assessment 1
✓ Audit Control 1-a
✓ Audit Control 1-b
✓ … …
Assessment 2
✓ Audit Control 2-a
✓ Audit Control 2-b
✓ … …

Source: AWS Audit Manager

USING AUDIT MANAGER TO ASSESS AWS RESOURCES

	PLANNING		*FIELDWORK*		
Audit/Assessment steps	Assessment objective and scope	Assessment initiation	Evidence collection	Evidence collection	REPORTING
Key Activities	• Understand the compliance requirements that the organization is subject to • Identify the AWS accounts, services, and resources that are in scope for the assessment	• Decide the assessment timelines (duration of evidence collection) • Initiate the assessment • Assign ownership for evidence gathering	• Continuous collection of evidence based on a defined frequency	• Review evidence gathered against applicable frameworks, standards and legal/regulatory requirements • Collate evidence in a format that is consumable by the reviewers	• Report the findings to the appropriate stakeholders
How does Audit Manager help?	• Provide a list of AWS resources and services that can be selected for the assessment	• Ability to select pre-built assessment frameworks • Ability to customize frameworks or add custom controls for the assessment • Ability to delegate or assign ownership of specific controls to individuals	• Supports automated collection of evidence daily • Preserve integrity of gathered evidence • Capture evidence metadata including source, timestamp, and status	• Collected evidence is converted into a consistent auditor friendly format • Assists in evidence assertion on some controls (Manual review of evidence for control assertion may be required	• Reports can be generated and accessed by relevant teams/personnel

Continuous compliance using Audit Manager

Continuous compliance

AWS Audit Manager supports continuous compliance by enabling compliance teams to collect and organize evidence continuously to help assess control compliance across AWS enterprise accounts. Customers can review and download reports and details for more than 2,600 security controls by using AWS Audit Manager.

The AWS Artifact portal provides on-demand access to AWS's security and compliance documents, including SOC reports, PCI reports, and certifications from accreditation bodies across geographies and compliance verticals.

Automated evidence collection

Auditing and monitoring controls are essential for meeting the requirements of each applicable regulatory framework. Auditing controls are technical safeguards that should be addressed through technical controls. Monitoring controls include procedures for monitoring logins and reporting discrepancies. A combination of services such as AWS Config, AWS CloudTrail and AWS Security Hub create a cost-effective solution for auditing and monitoring resources in the AWS environment. AWS Config provides an assessment and audit of configurations of various AWS resources, while AWS CloudTrail captures API calls made to an account (either through the command line, Software Development Kit (SDK) or through the console user interface). CloudTrail logs can also be directly ported to an Amazon S3 bucket for further analysis by a third-party security incident and event management (SIEM) solution.

Pre-built assessment frameworks

Compliance and audit functions typically struggle to manage compliance program focused on multiple regulatory requirements without significant efforts focused on creating common compliance approach. Audit Manager enables a more streamlined approach for organizations that are looking to remain compliant with multiple requirements with limited compliance overhead through pre-built assessment frameworks for commonly used control frameworks. By the very nature of these control frameworks, the scope of these controls may vary, and efforts to apply controls framework across the entire cloud environment may increase cost and time overhead.

Customizable control framework

Different organizations might have varied local, state, or federal regulatory requirements that they must comply with to protect their business's reputation and resources. In order to remain compliant, they must implement a specific set of controls. These controls can include organization's published policies and standards, documented procedures, and ongoing monitoring and assessment of controls.

Many organizations often struggle to carefully map internal controls for each audit scope against a complex, evolving set of compliance standards and legal agreements. For example, HIPAA requires organizations managing customer Protected Health Information (PHI) to produce evidence of proper handling of PHI. In addition, Sarbanes-Oxley (SOX) audits require evidence of effective change management for IT resources such as server or database configurations. Software licensing audits require evidence that licenses are used as authorized by the legal agreements.

Audit Manager can help simplify the effort for customers to map their organization specific internal controls against compliance standards and legal agreements by providing the capability to customize the control framework by adding controls specific to the organization's needs.

Granular scoping

Audit Manager provides users the ability to select specific resources/AWS services and AWS Accounts to be scoped in for the assessment, Audit Manager enables enterprises to enhance compliance efforts and focus only on assets that are part of the compliance scope.

Easily manageable workflows

Audit Manager provides an efficient way to track the chain of custody of all evidence reviewers to understand the source, who has access, and changes made to the evidence thus establishing accountability to the internal and external members involved in the process. It enables commenting and delegation for teamwork collaboration.

Audit integrity

In a distributed process, organizations may find it difficult to track the chain of custody of all evidence , to understand the source, who has access, and to track any changes. There arises a need to manage evidence, prevent tampering, and maintain accountability. Audit Manager can help you reduce the risk of evidence tampering and enables you to share assessment reports with confidence by using cryptographic verification. Audit Manager provides capabilities to manage user access privileges to control and restrict access to gathered evidence, and integrates with AWS Key Management Service to encrypt stored artifacts with customer managed keys.

Segregating access to the audit evidence

Depending on the purpose of the assessment/audit, the evidence could be relevant to different stakeholders within an organization (e.g., senior level executives, security team). To make sure the evidence is only being accessed by the team/individual it is meant for, Audit Manager allows for segregation assessments as per the least privilege model. Based on the role and responsibility assigned to the team/individual, they can be allowed to review and/or modify the assessment accordingly.

Centrally gather artifacts to provide to auditors

Managing evidence artifacts securely is one of the main challenges that compliance teams face daily. The varied nature of evidence and different stakeholders involved in capturing evidence only makes it challenging to keep evidence across different services, controls, and compliance frameworks consistent, easily usable, and cataloged. Evidence collected manually tends to provide only a point in time view of compliance and does not provide a confirmation of ongoing compliance to audit teams.

By leveraging the AWS global infrastructure, Audit Manager is a highly available, fault tolerant service that enables customers to scale their audit capability fast in the cloud as their business grows. Audit Manager makes it easier for customers to collect and organize evidence that is captured in daily evidence folders to support a view of continuous compliance. Using AWS Organizations with AWS Audit Manager allows you to run assessments over multiple accounts and consolidate evidence into a delegated administrator account. The resulting artifacts are secure and archived for safe record keeping, enhancing accountability and trust in the audit process. Also, by translating the evidences into a consistent readable format, Audit Manager speaks the auditors’ language.

Audit Manager aims to enhance the audit experience by increasing the effectiveness of controls in AWS while modernizing and simplifying the process

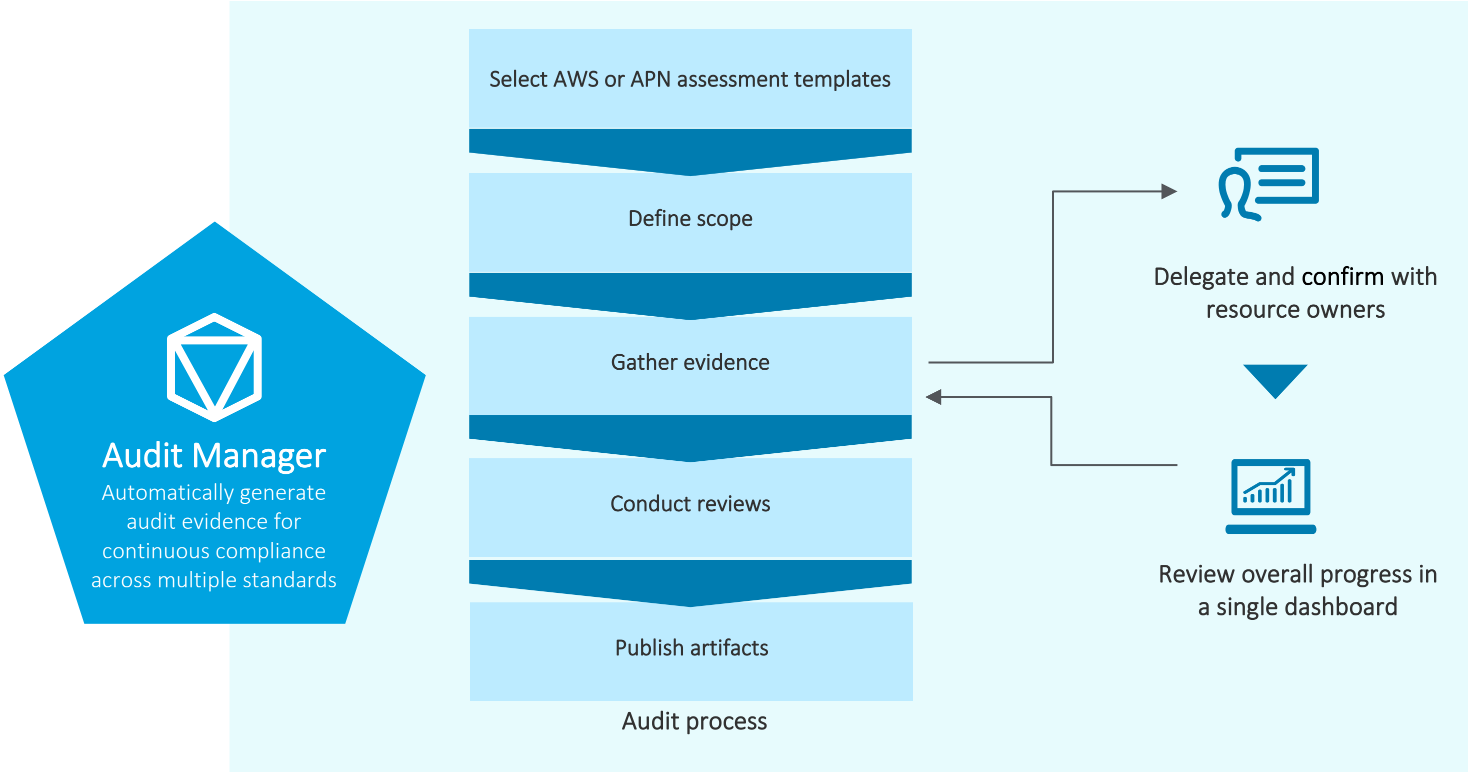
Leveraging Audit Manager efficiently

1. Determine the right Assessment Framework

The AWS Audit Manager allows users to continuously gather, track, and store evidence to help customers to audit their use of AWS services. Audit and GRC teams can collaborate in Audit Manager to review, curate, and finalize the evidence they want to publish as auditor-friendly artifacts, using cryptographic verification to avoid evidence tampering.

2. Define scope and specify/modify control statements

After finalizing the framework, the customer must select the list of AWS accounts under current region that need to be included in this audit assessment. Relevant AWS services (per assessment) will be selected by default in the summary list. Review the list and uncheck the services that should be out of scope for this assessment. Choose the members (i.e., process owners) of this assessment. Team members will have full visibility into the assessment content (e.g., controls status, evidence gathered).


Audit Manager
Automatically generate audit evidence for continuous compliance across multiple standards
Select AWS or APN assessment templates
Define scope
Gather evidence
Conduct reviews
Publish artifacts
Audit process
Delegate and confirm with resource owners
Review overall progress in a single dashboard

Source: AWS Audit Manager

3. Audit evidence collection process

Once launched, Audit Manager uses the mappings within an assessment to suggest relevant evidence already saved from past audits and continuously collect new evidence from AWS services for audit teams to review. Audit process owners can delegate assessment controls to team members to review evidence and enter remaining information needed to complete an assessment.

Audit Manager collects evidence from resource configurations, logs, and events from services such as AWS CloudTrail. Control findings and rule checks with pass/fail evaluation status from services such as AWS Security Hub, Config, and License Manager. Manual evidence that cannot be collected from the system and is uploaded by the customer.

4. Generate your reports and store securely

Once finalized, Audit Manager uses all the evidence in the assessment to produce encrypted reports with integrity check to prevent tampering. While the AWS Artifacts tells you if a particular service is compliant, Audit Manager validates whether the usage of the service on AWS is compliant.

Identify to Remediate

Identify gaps

Auditors and compliance teams can use AWS Audit Manager to identify control gaps against the control framework selected for the assessment. Control gaps can be identified using AWS Audit Manager through two approaches:

- For controls that are tagged as “Evaluation” controls, Audit Manager identifies the control gaps against the assessment requirements
- For other controls, Audit Manager identifies controls for which evidence captured from sources (such as AWS Config, CloudTrail) are inadequate

Risk rank gaps

Using an established risk ranking criteria, risk rank the identified gaps based on their priority and overall risk. Use the risk ranking of identified gaps to prioritize the remediation of the gaps identified.

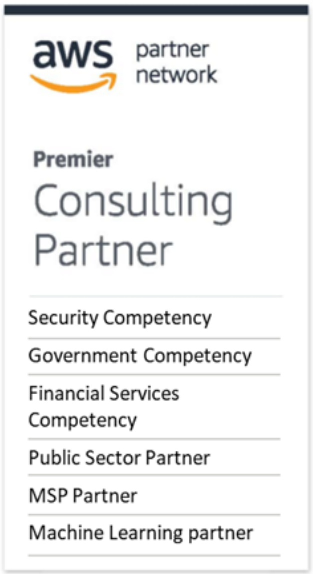
Plan remediation

AWS Audit Manager provides detailed remediation recommendations for each of the identified gap by providing links to AWS documentation and leading practices. Use the recommended remediation approach to plan the remediation of gaps identified.

Providing value at the intersection of risk, regulation, and AWS

- We are an APN Premier Consulting Partner and an AWS Security Competency Partner (Launch Partner)
- We have a dedicated Cloud Cyber Risk practice and relationships with AWS cloud security vendors
- Our cyber risk professionals have experience with design and implementation of secure AWS environments using DevSecOps
- Many of our services are built on AWS technologies, leveraging pre-built integrations that our clients can leverage to shorten time-to-value
- We have developed standard architecture patterns that enable a cloud-aware, end-to-end AWS security monitoring solution
- Our rich experience across a range of industry sectors guides focus on the regulations, standards, and cyberthreats that are likely to impact your business
- We have more than 3,100 cyber risk professionals in the US
- Part of a global team of 21,000 risk management and cyber risk professionals across the Deloitte Touche Tohmatsu Limited network of member firms

The strength of Deloitte/AWS relationship



aws partner network

Premier

Consulting Partner

Security Competency

Government Competency

Financial Services Competency

Public Sector Partner

MSP Partner

Machine Learning partner

Our relationship brings together Deloitte’s leadership in cyber and enterprise risk management with **the security-enabled cloud infrastructure of AWS**. In 2006, AWS began offering IT infrastructure services to businesses in the form of web services—now commonly known as cloud computing. Today AWS provides a highly **reliable, secure, scalable, low-cost** infrastructure that powers hundreds of thousands of businesses in 190 countries around the world, with **over a million active** customers spread across many industries and geographies.

Deloitte can help organizations adopt AWS securely and establish a security-first cloud strategy. Deloitte is an **AWS Premier Consulting Partner** and was one of the first eight organizations globally to achieve the **Security Competency** as a launch partner. Deloitte’s vast experience in Cyber Risk, combined with its extensive experience with AWS and Cloud technologies, enable us to provide **end-to-end** security solutions.

Deloitte & Touche LLP

Authors

Fiona Williams
Partner, Cyber Risk Services
AWS Alliance Leader
fwilliams@deloitte.com

Devendra Awasthi
Senior Manager, Cyber Risk Services
dawasthi@deloitte.com

Shar Qureshi
Senior Manager, Accounting & Internal Controls
shqureshi@deloitte.com

Manu Hoysala N
Manager, Cyber Risk Services
mhoysalan@deloitte.com

Mohideen Peer Mohamed
Manager, Cyber Risk Services
pmohideen@deloitte.com

Contributors

Shivi Srivastava
Consultant, Cyber Risk Services
shivisrivastava@deloitte.com

Sukant Khattar
Consultant, Cyber Risk Services
skhattar@deloitte.com

AWS

Kajal Deepak
General Manager, AWS Audit Manager
kajald@amazon.com

Ning Liu
Senior Product Manager, AWS Audit Manager
liunl@amazon.com

Steve Bollers
Senior Partner Solutions Architect, AWS
sboller@amazon.com

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

All product names mentioned in this document are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Deloitte & Touche LLP is not responsible for the functionality or technology related to the Vendor or other systems or technologies as defined in this document.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.