Service Name

AWS Audit Manager

Service Overview

AWS Audit Manager is a service that helps organizations continually audit their AWS usage to simplify how they assess risk and compliance with regulations and industry standards. Audit Manager automates evidence collection for policies, procedures, and activities (controls), making it easier to assess whether controls are operating effectively. The service provides prebuilt frameworks that structure and automate assessments for specific compliance standards or regulations, including a collection of controls with descriptions and testing procedures. When creating an assessment, Audit Manager automatically collects data from defined in-scope AWS accounts and transforms it into audit-friendly evidence for demonstrating compliance across security, change management, business continuity, and software licensing domains.

Key Use Cases

- Compliance Officers: Find non-compliant evidence across assessments and delegate remediation tasks to partner teams using evidence finder features
- Internal Risk Assessments: Support continuous auditing and compliance monitoring by automating evidence collection and maintaining audit readiness
- Multi-Account Evidence Management: Centrally manage and collect evidence from hybrid, multicloud, and multi-account AWS environments for comprehensive audit coverage

Features

- **Prebuilt Frameworks**: Gallery of frameworks supporting compliance standards like PCI DSS, HIPAA, SOC 2, GDPR, and AWS operational best practices
- **Automated Evidence Collection**: Continuous collection of evidence from AWS CloudTrail, AWS Config, AWS Security Hub, and API calls with configurable frequencies
- **Custom Controls and Frameworks**: Create custom controls from scratch or editable copies of existing controls to meet unique compliance requirements
- **Evidence Finder**: Search functionality to quickly find relevant evidence across all member accounts using filters and groupings
- **Delegation Workflow**: Assign control sets to subject matter experts for review, enabling cross-team collaboration in audit processes
- **Assessment Reports**: Generate audit-ready reports with evidence summaries and integrity validation through checksums

Value Proposition

AWS Audit Manager significantly reduces manual audit preparation effort by automating evidence collection and organizing it according to compliance requirements. The service saves thousands of hours typically spent manually collecting audit evidence, allowing teams to focus on risk remediation and audit planning:

- With prebuilt frameworks mapping AWS resources to control requirements for well-known standards, organizations can quickly establish audit readiness
- The delegation features enable efficient cross-team collaboration, while continuous evidence collection ensures ongoing compliance posture visibility
- Evidence integrity is maintained through secure, read-only storage with checksum validation, providing auditors with reliable, unaltered evidence for compliance assessments

Service Integration

AWS Audit Manager integrates deeply with multiple core AWS services for comprehensive evidence collection. AWS Security Hub provides automated security checks and compliance findings that Audit Manager captures as evidence snapshots:

- AWS Config supplies configuration compliance data and rule evaluations for resource assessments
- AWS CloudTrail delivers user activity logs that are continuously processed into audit evidence
- Additional integrations include AWS Organizations for multi-account assessments, AWS License Manager for software licensing compliance, AWS Control Tower for governance controls, and AWS Artifact for compliance documentation
- The service also connects with Amazon S3 for evidence storage and report generation, and supports integration with third-party GRC systems through APIs

Onboarding and Offboarding

Getting started requires completing account prerequisites including AWS account setup, creating administrative users, and granting necessary IAM permissions. Customers enable Audit Manager through the console, CLI, or API, with options for custom encryption keys and delegated administrator accounts:

- Recommended setup includes enabling AWS Organizations for multi-account assessments, AWS Security Hub for security findings, and AWS Config for compliance checks
- The onboarding process involves selecting from prebuilt frameworks or creating custom ones, specifying assessment scope across AWS accounts, designating audit owners, and initiating evidence collection

- First-time users should review Audit Manager concepts, complete the tutorial for creating assessments, and configure recommended integrations with supporting services

Getting Started Guide: https://docs.aws.amazon.com/audit-manager/latest/userguide/getting-started.html

Data Removal

Data removal occurs through multiple mechanisms: automatically when disabling the service, after a two-year retention period in managed storage repositories, or manually by deleting individual resources. Service metadata is encrypted at rest using AWS owned keys, while customer content uses either customer-managed or AWS owned keys. Evidence data is stored in Audit Manager's managed repository with read-only permissions, and assessment reports are saved to customer S3 buckets for additional control over data lifecycle management.

Backup/Restore and Disaster Recovery

AWS Audit Manager stores evidence in its own managed storage repository with built-in durability and availability. Evidence data is retained for up to two years with automatic deletion thereafter. Assessment reports are generated and stored in customer-specified S3 buckets, allowing customers to leverage S3's backup and versioning capabilities. The service does not provide native backup features but relies on AWS infrastructure resilience and customer-controlled S3 storage for report preservation and recovery scenarios.

Backup Capabilities

AWS Audit Manager does not have dedicated backup capabilities and does not integrate with AWS Backup service. The service maintains evidence in managed storage repositories with built-in durability, but customers must rely on S3 storage for assessment reports and implement their own backup strategies for critical compliance documentation. Evidence integrity is maintained through checksums and secure storage rather than traditional backup mechanisms.

Disaster Recovery

AWS Audit Manager does not integrate with AWS Elastic Disaster Recovery service. The service operates as a regional service ensuring evidence collection remains within regional boundaries:

- Disaster recovery relies on AWS infrastructure resilience and the distributed nature of evidence collection from multiple AWS services
- Customers must enable Audit Manager in each region separately and cannot aggregate evidence across regions, requiring region-specific disaster recovery planning

Recovery Objectives

AWS Audit Manager supports RPO objectives through continuous evidence collection from integrated services like CloudTrail, Config, and Security Hub, ensuring minimal data loss in compliance tracking. RTO objectives are supported by the service's regional architecture and integration with resilient AWS services. However, recovery depends on underlying AWS service availability and evidence collection resumption rather than specific RPO/RTO guarantees from Audit Manager itself.

Service Constraints

Service Quotas: https://docs.aws.amazon.com/audit-manager/latest/userguide/service-quotas.html

FAQ: https://aws.amazon.com/audit-manager/faqs/

Technical Requirements

Service Documentation: https://docs.aws.amazon.com/audit-manager/latest/userguide/what-is.html

User Guide: https://docs.aws.amazon.com/audit-manager/latest/userguide/what-is.html

API Reference: https://docs.aws.amazon.com/audit-manager/latest/APIReference/Welcome.html

Pricing Overview

Please see the AWS UK G Cloud 15 Pricing Document accompanying this service in the Digital Marketplace.

Public Pricing: https://aws.amazon.com/audit-manager/pricing/

Cost Optimization

AWS Audit Manager offers a free tier providing 35,000 resource assessments per month for two calendar months for first-time customers. Cost optimization strategies include carefully scoping assessments to necessary accounts and resources to minimize resource assessment charges:

- Organizations can optimize costs by using common controls across multiple frameworks, leveraging shared custom frameworks across accounts and regions, and strategically scheduling evidence collection frequencies (daily, weekly, monthly) based on compliance requirements
- The evidence finder feature incurs additional CloudTrail Lake charges, so selective enablement based on search needs can control costs

Savings Considerations

Primary cost savings come from reduced manual audit preparation effort, potentially saving thousands of hours in evidence collection and organization. The automated evidence collection eliminates need for dedicated staff to manually gather compliance documentation:

- Using prebuilt frameworks reduces custom development costs compared to building compliance systems from scratch
- Multi-account evidence consolidation reduces operational overhead across large organizations
- However, customers should monitor resource assessment volumes as the primary cost driver, optimize assessment scope to essential resources, and leverage the free tier for initial evaluation and smaller workloads to maximize cost efficiency