AWS Decision Guide

Choosing an AWS cloud governance service

Choosing an AWS cloud governance service: AWS Decision Guide

Table of Contents

Decision guide 1
Introduction 1
Understand 2
Consider 3
Choose 5
Use 8
Explore 12
Document history 14

Choosing an AWS cloud governance service

Taking the first step

Purpose	Help determine which AWS cloud governance services are the best fit for your organization.
Last updated	October 4, 2024
Covered services	• AWS Artifact • AWS Audit Manager • AWS CloudFormation • AWS CloudTrail • AWS Config • AWS Control Tower • AWS Organizations • AWS Security Hub • AWS Service Catalog • AWS Systems Manager • AWS Trusted Advisor

Introduction

Cloud governance is a set of rules, processes, and reports that helps you align your AWS Cloud use toward your business objectives.

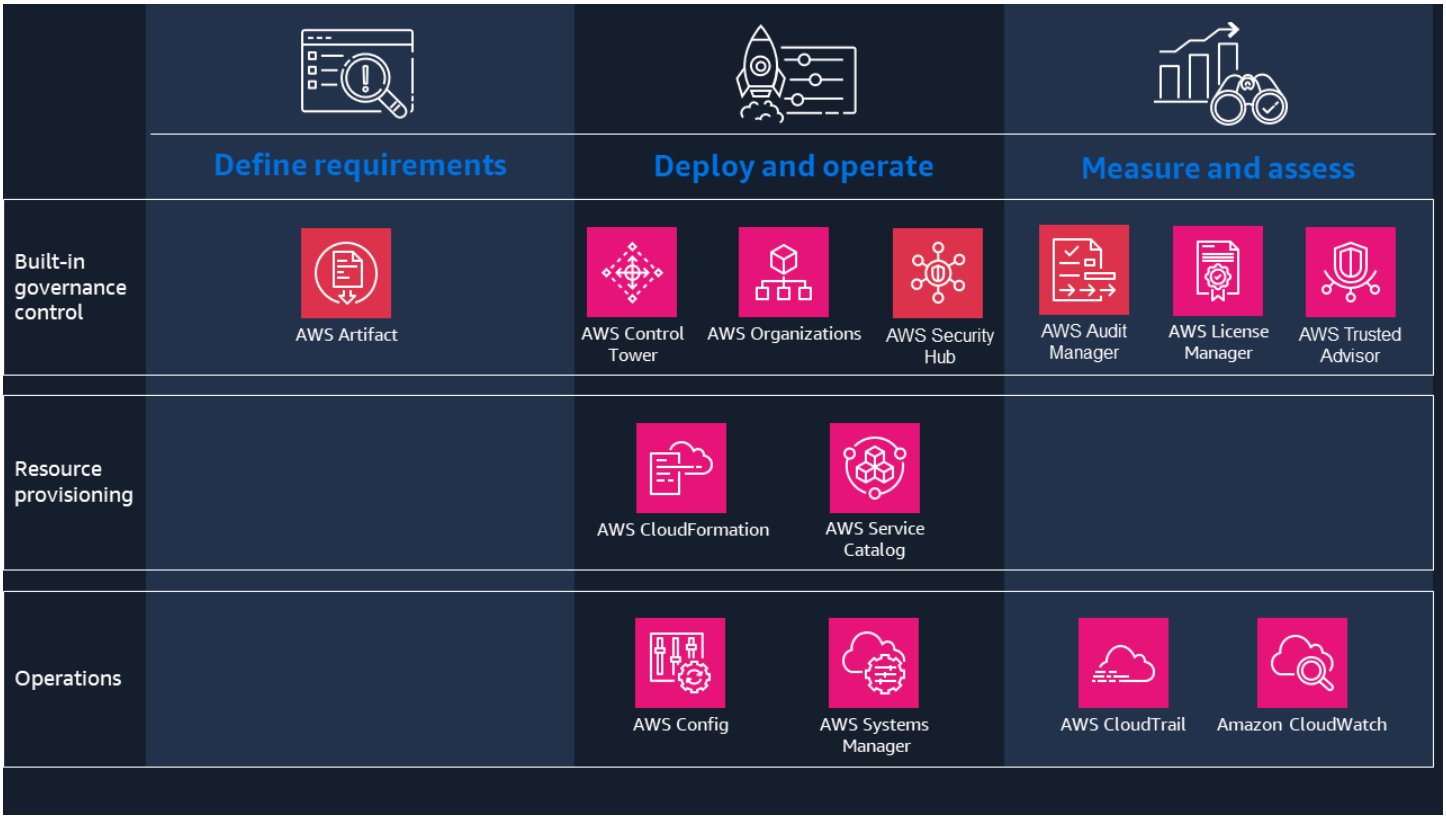
This covers security, by enabling multi-account strategies, continuous monitoring, and control policies. It covers compliance, by automating checks, reporting, and remediation. It covers operations, by applying controls enterprise wide. It covers identity by centralizing identity and access management at scale. It covers cost, by facilitating usage reports and policy enforcement. And it covers resilience, by helping integrate assessments and testing into CI/CD pipelines for validation.

We offer a range of services to help you set up, manage, monitor, and control the use of accounts, services, and resources in the cloud, thereby implementing cloud governance best practices.

The guide is designed to help you decide which AWS cloud governance services are the best fit for your organization, to strengthen operational resilience, optimize costs, and build controls to help comply with regulations or corporate standards, while maintaining development speed and accelerating innovation.

This video is a six-minute segment of a presentation introducing best practices for cloud governance.

Understand



The previous diagram shows how cloud governance draws on multiple AWS services, which allow you to define your governance requirements, deploy and operate your systems, and measure and assess their performance. The services provide built-in governance control, resource provisioning to align with your governance policies, and operations tools to help you monitor and manage your environment.

Harnessing AWS cloud governance services helps you ensure your cloud use supports your business objectives, Specifically, they enable you to improve speed and agility for developers, operate in a dynamic regulatory environment, streamline mergers and acquisitions, and strengthen operational resilience:

- **Improve speed and agility for developers —** Quickly spin new environments through APIs making sure your developers are not waiting on weeks long provisioning cycles, and accelerate provisioning of CI/CD pipeline. Find and prevent defects early in the software delivery process, using pre-built controls and rules, and infrastructure-as-code templates for provisioning common resources efficiently.
- **Operate in a dynamic regulatory environment —** Create always-on boundaries to protect and control access to data across AWS, codify your compliance requirements, and automate the assessment of your resource configurations across your organization.
- **Streamline mergers and acquisitions —** Migrate workloads faster by building a secure, well-architected, multi-account environment. Centralize account creation, allocate resources, group accounts, and apply governance policies and controls easily and quickly. Adopt a programmatic approach to multi-account management at scale.
- **Strengthen operational resilience —** Set up a secure, well-architected, resilient multi-account environment quickly. Run assessments of your workloads to uncover potential resilience-related weaknesses. Conducts automated checks against five key areas – cost optimization, performance, security, fault tolerance, and service limits – and receive recommendations that enable you to follow known best practices.
- **Optimize costs —** Visualize, understand, and manage costs and usage over time. Continuously analyze resource utilization, identify underutilized resources, and terminate idle resources.

Cloud governance best practices can effectively be built in when you set up and operate your workloads on AWS. Interoperable services help you achieve consistent, centralized governance over your IT estate, including AWS and third-party products. Breadth and depth of controls across AWS services help you meet evolving regulatory requirements and minimize security risks.

Consider

The following section outlines some of the key criteria to consider when choosing a cloud governance strategy. In particular, it discusses the different kinds of cloud environment, control regime, and developer support opportunities that might be applicable to your organization and business objectives.

Multi-account strategy

> **What it is:** Implementing cloud environment best practices hinges on adopting a secure multi-account strategy. Use accounts as building blocks, and group them into organizational

units (OUs), such as foundational OUs for security and infrastructure, and additional OUs for sandboxing and workloads.

Why it matters: A multi-account strategy provides natural boundaries and isolation in your cloud environment. This in turn allows you to manage quotas and account limits, automate the provisioning and customization of accounts, and apply the principle of least privilege by restricting access to your management account. It enables visibility to track user activity and risk across your environment. Your multi-account strategy acts as the foundation on which you can build for migration projects or organizational changes like mergers and acquisitions.

Use AWS Organizations to consolidate multiple AWS accounts into an organization, which you can use to allocate resources, group accounts, and apply governance policies.

Use AWS Control Tower as an orchestration service, layered on top of AWS Organizations, to help structure your AWS estate, and extend governance over OUs and your multi-account environment.

Controls management best practices

What it is: Implementing controls management best practices can include a range of approaches. Detective controls catch resources that violate defined security policies. Preventive controls protect security baselines by blocking specific actions. And proactive control scan resources before they are provisioned, stop non-compliant code from being deployed, and instruct developers to remediate them. Interoperable AWS services give you centralized governance and control over your entire IT estate, including AWS and third-party products, as you grow into new markets.

Why it matters: Controls management best practices allow you to programmatically implement controls at scale, and automatically configure compliance or remediate non-compliance. This is particularly important if your organization operates in a regulated industry, such healthcare, life sciences, financial services, or the public sector, where specific regulatory frameworks apply, or adheres to specific corporate standards, or data residency and digital sovereignty requirements.

Consider opportunities for orchestrating multiple AWS services to ensure your organization's security and compliance needs, using AWS Control Tower, defining configuration settings and detecting deviation from them, using AWS Config, and auditing AWS usage and compliance with regulations and industry standards, with AWS Audit Manager.

Cloud governance for developers

What it is: Implementing cloud governance best practices for developers can include using infrastructure as code (IaC) to ensure repeatability and consistency in their work, and establishing processes to detect security vulnerabilities.

Why it matters: This helps teams move fast while being confident in their governance processes. It gives developers a single source of truth that can be deployed to the whole stack, infrastructure that they can replicate, redeploy, and repurpose, the ability to control versioning on infrastructure and applications together, and a choice of self-service actions.

Cloud governance for developers can also involve detecting security vulnerabilities in code. This helps them improve code quality, identify critical issues, ensure consistent release pipelines, and launch projects with blueprints.

Consider how you might provide builders with pre-approved infrastructure-as-code templates, and corresponding IAM policies that dictate who, where, and how they can be used, using an AWS service like Service Catalog.

Scalability and flexibility

What it is: Choose AWS services that will help your cloud governance measures grow seamlessly with your infrastructure and adapt to evolving requirements. Consider how your organization will grow, and how fast.

Why it matters: Considering scalability and flexibility helps you ensure that your cloud governance arrangements are robust, responsive, and capable of supporting dynamic business environments.

To help you scale quickly, AWS Control Tower orchestrates the capabilities of several other AWS services, including AWS Organizations and AWS IAM Identity Center, to build a landing zone in less than an hour. Control Tower sets up and manages resources on your behalf.

AWS Organizations enables you to manage 40+ services' resources across multiple accounts. This gives individual application teams the flexibility and visibility to manage cloud governance needs that are specific to their workload, while also giving them visibility to centralized teams.

Choose

Now you know the criteria by which you will be evaluating your cloud governance options, you are ready to choose which AWS cloud governance service may be a good fit for your organizational

needs. The following table highlights which services are optimized for which circumstances. Use it to help determine the service that is the best fit for your organization and use case.

Type of use case	When would you use it?	Recommended service
Defining requirements	To provide on-demand downloads of AWS security and compliance documents.	AWS Artifact
Deploying and operating	To speed up cloud provision ing with infrastructure as code.	AWS CloudFormation
	To represent your ideal configuration settings and detect if AWS resources drift from it.	AWS Config
	To setup and orchestrate multiple AWS services on your behalf while helping you meet the security and compliance needs of your organization.	AWS Control Tower
	To consolidate multiple AWS accounts into an organization, which you can use to allocate resources, group accounts, apply governance policies, and manage centrally and at scale.	AWS Organizations
	To run automated and continuous checks against the rules in a set of supported security standards.	AWS Security Hub

Type of use case	When would you use it?	Recommended service
	To provide builders with pre-approved infrastructure-as-code templates, and corresponding IAM policies, that dictate who, where, and how they can be used.	Service Catalog
	To provide secure end-to-end management of resources on AWS and in multicloud and hybrid environments.	AWS Systems Manager
Measuring and assessing	To audit AWS usage and assess risking and compliance with regulations and industry standards.	AWS Audit Manager
	To enable operational and risk auditing, governance, and compliance of your AWS account.	AWS CloudTrail
	To monitor your AWS resources and the applicati ons you run on AWS in real time.	Amazon CloudWatch
	To manage software licenses from vendors centrally across AWS and your on-premises environments.	AWS License Manager
	To evaluate usage and configuration against best practices.	AWS Trusted Advisor

Use

You should now have a clear understanding of what each AWS cloud governance service does, and which ones might be right for you.

To explore how to use and learn more about each of the available AWS cloud governance services, we have provided a pathway to explore how each of them works. The following sections provide links to in-depth documentation, hands-on tutorials, and other resources to get you started.

AWS Artifact

- **Getting started with AWS Artifact**

  Download security and compliance reports, manage legal agreements, and manage notifications.

  Explore the guide »

- **Managing agreements in AWS Artifact**

  Use the AWS Management Console to review, accept, and manage agreements for your account or organization.

  Explore the guide »

- **Prepare for an Audit in AWS Part 1 – AWS Audit Manager, AWS Config, and AWS Artifact**

  Use AWS services services to help you automate the collection of evidence that's used in audits.

  Read the blog »

AWS Audit Manager

- **Getting started with AWS Audit Manager**

  Enable Audit Manager by using the AWS Management Console, the Audit Manager API, or the AWS CLI.

  Explore the guide »

- **Tutorial for Audit Owners: Creating an assessment**

Create an assessment by using the Audit Manager Sample Framework.

Get started with the tutorial »

- **Tutorial for Delegates: Reviewing a control set**

  Review a control set that was shared with you by an audit owner in Audit Manager.

  Get started with the tutorial »

AWS CloudTrail

- **View event history**

  Review the AWS API activity in your AWS account for services that support CloudTrail.

  Get started with the tutorial »

- **Create a trail to log management events**

  Create a trail to log management events in all Regions.

  Get started with the tutorial »

AWS Config

- **AWS Config features**

  Explore the resource tracking capabilities of AWS Config, from configuration histories and snapshots to customizable rules and conformance packs.

  Explore the guidance »

- **How AWS Config Works**

  Dive deeper on AWS Config, and learn how the service discovers and tracks resources, and delivers configuration items through various channels.

  Explore the guide »

- **Risk and Compliance workshop**

  Automate controls by using AWS Config and AWS Managed Config Rules.

Explore the workshop »

- **AWS Config Rule Development Kit library: Build and operate rules at scale**

  Use the Rule Development Kit (RDK) to build a custom AWS Config rule and deploy it with the RDKLib.

  Read the blog »

AWS Control Tower

- **Getting started with AWS Control Tower**

  Learn how to set up your landing zone using the AWS Control Tower console or APIs.

  Explore the guide »

- **AWS Control Tower controls management workshop**

  Learn how to set up governance on your multi-account environment to align with AWS best practices and common compliance frameworks.

  Explore the workshop »

- **Modernizing Account Management with Amazon Bedrock and AWS Control Tower**

  Provision a security tooling account and leverage generative AI to expedite the AWS account setup and management process.

  Read the blog »

- **Building a well-architected AWS GovCloud (US) environment with AWS Control Tower**

  Set up your governance in the AWS GovCloud (US) Regions, including governing your AWS workloads by using Organizational Units (OUs) and AWS accounts.

  Read the blog »

AWS Organizations

- **Getting started with AWS Organizations**

Learn how to start using AWS Organizations, including reviewing terminology and concepts, using consolidated billing, and applying organization policies.

Explore the guide »

- **Creating and configuring an organization**

  Create your organization and configure it with two AWS member accounts.

  Get started with the tutorial »

- **Organizing Your AWS Environment Using Multiple Accounts**

  Learn how using multiple AWS accounts can help isolate and manage your business applications and data, and optimize across the AWS Well-Architected Framework pillars.

  Read the whitepaper »

- **Services that work with AWS Organizations**

  Understand which AWS services services you can use with AWS Organizations and the benefits of using each service on an organization-wide level.

  Explore the guide »

- **Best Practices for Organizational Units with AWS Organizations**

  Dive deep into the recommended architecture of AWS best practices when building your organization, for OU structure and specific implementation examples.

  Read the blog »

- **Achieving operational excellence with design considerations for AWS Organizations SCPs**

  Learn how SCPs help control access to AWS services and resources provisioned across multiple accounts created within an organization.

  Read the blog »

AWS Security Hub

- **Enabling AWS Security Hub**

  Enable AWS Security Hub with AWS Organizations or in a standalone account.

Explore the guide »

- **Cross-Region aggregation**

  Aggregate AWS Security Hub findings from multiple AWS Regions to a single aggregation Region.

  Explore the guide »

- **AWS Security Hub workshop**

  Learn how to use AWS Security Hub and to manage and improve the security posture of your AWS environments.

  Explore the workshop »

- **Three recurring Security Hub usage patterns and how to deploy them**

  Learn about the three most common AWS Security Hub usage patterns and how to improve your strategy for identifying and managing findings.

  Read the blog »

Explore

Architecture diagrams

Explore reference architecture diagrams to help you develop your security, identity, and governance strategy.

Explore architecture diagrams

Whitepapers

Explore whitepapers for more insights and best practices on choosing, implementing, and using the security, identity, and governance services that best fit your organization.

Explore whitepapers

Solutions

Use these solutions to further develop and refine your security, identity, and governance strategy.

Explore solutions

Document history

The following table describes the important changes to this decision guide. For notifications about updates to this guide, you can subscribe to an RSS feed.

Change	Description	Date
Initial publication	Guide first published.	October 4, 2024