Cloud Governance: Driving Success and Security in the Cloud

Creating a robust cloud governance strategy with the support of AWS and AWS security competency partners
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safeguarding your business means governing your cloud</td>
<td>3</td>
</tr>
<tr>
<td><strong>Visibility:</strong> you can’t govern what you can’t see</td>
<td>4</td>
</tr>
<tr>
<td><strong>Configuration:</strong> setting the stage for success</td>
<td>5</td>
</tr>
<tr>
<td><strong>Operations:</strong> managing the processes that manage your cloud</td>
<td>6</td>
</tr>
<tr>
<td><strong>Risk:</strong> where governance meets the bottom line</td>
<td>7</td>
</tr>
<tr>
<td><strong>Better together:</strong> cloud governance takes all of us</td>
<td>8</td>
</tr>
<tr>
<td>Cloud success and security start now</td>
<td>9</td>
</tr>
</tbody>
</table>
Safeguarding your business means governing your cloud

What do all these real-life situations have in common?

- A company discovered that customers' credit card data was posted in an unprotected notes field on a custom cloud-based application, violating PCI.
- A business learned that some of its valuable IP was visible on publicly accessible infrastructure.
- A company realized that it failed to protect a server with a password, leaving a database of customer information unprotected.
- An organization discovered a misconfiguration that left it open to data breach.

All of these organizations—and dozens more like them in a variety of industries, including highly regulated ones like finance and healthcare—had a cloud computing strategy that took advantage of cloud benefits, but left out a critical component: cloud governance.

In practical terms, a robust cloud governance strategy helps you run your business well and keep it safe, offering a level of protection against a number of avoidable risks: data breaches, intellectual property theft, damage to brand and reputation, and financial loss, as well as the risk of being out of compliance with mandates like PCI and HIPAA. In fact, Gartner, the leading IT research and advisory firm, predicts that “through 2025, 99% of cloud security failures will be the customer’s fault.”

Creating effective cloud governance is a two-step process:

1. Understanding the four pillars of cloud governance: visibility, configuration, operations, and risk.
2. Developing best practices for continuously monitoring, assessing, and optimizing each of these.

Read on to learn how Amazon Web Services (AWS) and AWS Partners can help you create the cloud governance strategy you need to safeguard your business and drive your success.

What is cloud governance?

Cloud governance enables customers to define requirements for security, cost, and ongoing oversight of their cloud journey and ensure processes are optimized and consistently followed.

A robust cloud governance strategy helps you run your business well and keep it safe.

---

Visibility: you can’t govern what you can’t see

In terms of cloud governance, visibility means having an accurate, detailed, and up-to-date view of all the activity an organization has in the cloud. Practically speaking, that includes:

- Cloud assets such as applications, platforms, infrastructure, VPC, buckets, etc.
- AWS accounts
- Data stored in the AWS Cloud
- Roles and/or users and specific data they can access

Although this sounds straightforward, it’s actually quite challenging, particularly in a hybrid or multi-cloud environment or in a distributed global organization with multiple users, departments, and groups. In these environments, it’s especially easy for unmanaged IT to proliferate—which includes the use of IT-related hardware, software, and services by a department or individual without the knowledge of the organization’s IT department or security group. By definition, unmanaged IT is invisible, and therefore ungovernable.

AWS services designed to support visibility across cloud environments can help.

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect AWS accounts, workloads, and data stored in Amazon S3.

Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect sensitive data in AWS, something that becomes increasingly challenging as data volumes grow.

AWS Security Hub provides a comprehensive view of an organization’s security alerts and security posture across AWS accounts by aggregating, organizing, and prioritizing security alerts or findings from multiple AWS services (including Amazon Macie) in a single place.

AWS CloudTrail allows users to log, continuously monitor, and retain account activity related to actions across the AWS infrastructure, providing a comprehensive event history that simplifies security analysis, resource change tracking, and troubleshooting.

More AWS visibility solutions:

- AWS Config
- Amazon CloudWatch
- AWS APIs

Amazon Partners also offer validated solutions that help organizations improve their cloud visibility, as well as manage configuration, operations, and risk. AWS Partners leverage and integrate with AWS services to build unique solutions that enable businesses to take full advantage of all AWS has to offer at every stage of their cloud journey.
When talking about cloud governance, configuration is most often thought of in terms of misconfiguration—errors or oversights in configuration that violate an organization’s configuration policy or allow unintended behaviors that impact system security. A typical example involves user permissions and controls, where an unauthorized individual is inadvertently given access to sensitive data or the ability to make system changes beyond the scope of his or her responsibilities.

Misconfigurations also pose a major risk when it comes to meeting compliance mandates in regulated industries like healthcare and finance (for example, HIPAA and PCI) or complying with regulations like General Data Protection Regulation (GDPR).

Misconfigurations pose a major risk when it comes to meeting compliance mandates.

A robust cloud governance strategy requires a process for finding, addressing, and tracking misconfigurations on a continuous basis to ensure compliance at scale. AWS services can help:

- **AWS Foundational Security Best Practices standard** is a set of controls that detects when deployed accounts and resources deviate from security best practices. The standard provides actionable and prescriptive guidance on how to maintain and improve organizational security posture.

- **AWS Config Conformance Packs** provide a collection of AWS Config rules and remediation actions that can be easily deployed as a template to evaluate an organization’s AWS environment.

- **AWS IAM Access Analyzer** helps organizations identify the resources or accounts, such as Amazon Simple Storage Service (Amazon S3) buckets or identity and access management (IAM) roles, that are shared with an external entity, uncovering instances of unintended access to resources and data.
As companies scale up their investment in cloud computing, adding people, processes, and technology to the mix, it’s not uncommon to find that the **operations** designed to manage those activities haven’t kept up. Manual processes and homegrown solutions that once worked well become nearly impossible to manage and maintain at scale, opening the door to non-compliance and other risks.

A robust cloud governance strategy requires the development of automated processes that detect, report, and remediate operational issues. However, while these processes should be automated, remediation efforts should not. Instead, policies and prescriptive guidance should be developed that proactively prevent violations whenever possible. An effective approach integrates operational change management processes into DevOps workflows. This includes automated governance controls to ensure consistent compliance, as well as preventative guardrails in the deployment pipeline to limit non-compliant actions.

**As you deploy policies and procedures to more effectively and securely manage your operations in the cloud, AWS can help.**

- **AWS Systems Manager** provides a unified user interface that allows organizations to view operational data from multiple AWS services and automate operational tasks across AWS resources. Systems Manager simplifies resources and application management, shortens the time to detect and resolve operational problems, and makes it easy to operate and manage infrastructure at scale.

- **AWS Control Tower** provides the easiest way to set up and govern a secure, multi-account AWS environment, ensuring that all accounts conform to company-wide policies through built-in best practices.

- **AWS Organizations** helps users centrally manage and govern their environment as they grow and scale AWS resources.

**More AWS Operations solutions:**

- Amazon GuardDuty
- Amazon EventBridge
- AWS Security Hub
- AWS APIs
- AWS CloudFormation

Manual processes and homegrown solutions become nearly impossible to manage at scale, opening the door to non-compliance and other risks.
Risk: where governance meets the bottom line

When organizations think about cloud governance, the assessment, management, and mitigation of risk is often the first thing that comes to mind. But there are many different kinds of risks, ranging from data security, regulatory risk, financial risk, and shadow IT. What all these risks have in common is their potential to significantly damage your organization’s financial position, compliance posture, customer confidence, and brand or reputation.

Processes are needed to find, address, and reduce security risks at scale. This includes optimizing cloud resources to reduce the likelihood of data breaches, system vulnerabilities, and errors in identity authentication and access management. In addition, artificial intelligence can increase visibility into critical events and provide real-time information to help manage risk.

AWS services can help assess, manage, and mitigate risk throughout the cloud.

AWS Audit Manager continuously audits AWS usage to simplify how organizations assess risk and compliance with regulatory standards. AWS Audit Manager automates evidence collection and enables audit capability in the cloud to scale as needed. AWS Audit Manager makes it easy for companies to assess whether their policies, procedures, and activities are operating efficiently.

AWS Config provides the means to assess, audit, and evaluate AWS resource configurations. AWS Config continuously monitors and records those configurations, automating the evaluation of recorded configurations against desired configurations. With AWS Config, organizations can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine overall compliance against internal guidelines, simplifying compliance auditing, security analysis, change management, and operational troubleshooting.

There are many different kinds of risks, and all have the potential to significantly damage your organization.
Better together: cloud governance takes all of us

Cloud governance is based on a shared responsibility model, in which both AWS and your organization share the responsibility for data security and compliance.

AWS is responsible for the security OF the cloud. That means AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS cloud, which includes the hardware, software, networking, and facilities that run AWS cloud services.

Your organization is responsible for security IN the cloud. Your responsibility is determined by the AWS cloud services you select, which then determines the amount of configuration work you must perform as part of your security responsibilities. Your organization is responsible for:

- the security of your data
- platform, applications, identity, and access management
- operating system, network, and firewall configuration
- client-side, server-side, and networking traffic encryption and protection

When it comes to managing your portion of the shared responsibility model, you don’t have to go it alone: AWS partners provide complementary capabilities that help organizations meet their security and compliance responsibilities. Partners offer integration and support services that help throughout the migration process.
Cloud success and security start now

Is your organization ready to take the next step on its cloud governance journey? Ask yourself:

- Do we have full visibility into our cloud infrastructure?
- Can we easily and effectively find and remediate misconfigurations?
- Do we have automated processes for managing cloud operations?
- Can we find, address, and reduce risks at scale?

If you answered “no” to any of these questions (or even if you’re unsure), it’s easy to find out more. Visit the AWS Security Competency Partners page to learn about security-focused solutions for your specific workloads and use cases, You’ll also find partners offering a complimentary cloud security risk assessment.