GETTING STARTED WITH GOVERNANCE AND COMPLIANCE FOR AWS

Among its many benefits, the Amazon Web Services (AWS) ecosystem offers end users assuredness that governance principles are being upheld and risks associated with operating on the cloud are minimized. However, enterprise leaders are still responsible for the security and compliance of their data and applications in the cloud.

Below, we will examine how AWS includes governance and compliance provisions to its multi-functional cloud platform for enterprise businesses.

(This tutorial is part of our AWS Guide. Use the right-hand menu to navigate.)

Governance & Compliance Overview

Due to advances in monitoring and automation and the vast resources available departmentally, the IT team in an enterprise organization usually has governance and compliance processes folded into their daily activities.

To understand the capabilities of governance and compliance within AWS, it's first important to understand what is meant by each term:

- **Governance** refers to the body of oversight that sets standards to reduce business risk. Said another way, governance has to do with the processes, mission, values and metrics that a company must meet to ensure efficient use of IT functions.Governance bodies vary by industry sector and location. One governing body that sets international standards of governance and

leadership across industries is the International Organization for Standardization (ISO). AWS is ISO 27001 certified; however this only covers the AWS side of Amazon's shared responsibility model (more on this soon).

- **Compliance** is the act of mitigating risks by strict IT adherence to governance standards; including provisioning and configuring resources and monitoring compliance issues. This includes tasks like monitoring compliance dashboards and running reports for stakeholders, reducing business risk by ensuring data security and more. Within this space, IT teams must:
  - ***Define*** compliance resources
  - ***Uncover*** new resources for remaining compliant
  - ***Monitor*** enterprise compliance with universal and organizational standards
  - ***Manage*** compliance data, including reporting and responding to issues

The challenge becomes a time and resource management issue. When IT employees become entrenched in what might seem like "compliance busy work" productivity and innovation is diminished in the area where IT teams should shine: development of new applications, workflows and processes.

AWS is one answer to overcoming this dilemma by allowing teams to manage and monitor compliance without compromising agility. By design, the platform allows users to define configuration and provisions, uncover new resources and changes made to existing ones, monitor, manage and report on compliance.

The Challenge: Governance Strategy on AWS

One way that AWS accelerates application deployment is by offering end users a managed services approach to governance through automation.

But before automation can be a real option for enterprise organizations they must accomplish some baseline feats of understanding. This includes being aware of compliance needs and adapting to governance standards, setting up a basic framework with stakeholders and knowledge of AWS shared responsibility model.

Defining a Governance Strategy

First and foremost, end users need to have a governance strategy in place if they are going to successfully implement governance and compliance on AWS. This includes selecting a framework and identifying stakeholders.

- A framework: refers to the IT principles that drive innovation throughout the enterprise organization
- Key stakeholders: are individuals responsible for implementing a framework that reduces business risk

Understanding Compliance Requirements

The next important thing to understand is your own organization's compliance requirements. You won't be able to create the framework necessary for compliance in AWS without them.

Common compliance standards come from these organizations:

- DoD Cloud Security Model
- FedRAMP
- HIPPA
- ISO 27001
- NIST SP 800-53
- PCI DSS

While these are typical in the United States, this is just the tip of the iceberg when it comes to standards agencies. Around the world, there are many international, regional and industry-specific organizations that offer guidelines, tips and framework solutions for governance and compliance.

Architectural Challenges

One criticism of AWS is that it has a steep learning curve. Amazon offers possibly the most reliable and comprehensive open source development ecosystem available to consumers today. At the same time, the AWS culture of innovation and continuous development means that there is an overwhelming number of resources for IT architects to choose from when building a framework based on their governance strategy.

The endless possibilities can seem daunting, and that leaves room for error. To lay the groundwork for automation and reduce chances for architectural error, it's imperative to implement a governance model that is organized like a managed services solution.

Here's how:

A Managed Services Governance Solution

At the core of a governance model that operates like a managed services solution is AWS shared responsibility. Enterprise organizations should assign a layer of governance between the security provided by AWS and that completed by the assigned end users.

In essence, AWS is responsible for securing the cloud server and the end user is presumably responsible for securing everything else from basic customer data to back end functions like monitoring and billing.

In a managed services-type model teams of Managed Services Operators (MSOs) remove some of the operational burden from the end user by securing back end functionality, leaving the end user to secure only customer data and applications they access and use daily.

Typical MSO Responsibilities

Assigning the right people to be MSOs is a key part of this approach. Overall, according to AWS, an MSO "provides the minimum requirements for workload owners who are deploying applications in the cloud."

Typical responsibilities in the MSO role include:

- Security and continuous monitoring
- Management and reporting
- Assigning provisions and configurations (Amazon VPC and IAM)
- Designing approved templates

- Creating common machine images
- Development of MSO VPC which includes logging endpoints, access management, platform management, shared services and more

MSOs should have a strong development background and understanding of cloud development, as well as experience with management and organizational oversight.

Architectural Baselines Approach

The MSO teams will also set architectural baselines. Using this approach, teams strive to ensure automation works every time by establishing certain workload baselines throughout the enterprise.

These architectural baselines will be frameworks built with existing compliance and governance best practices and standards for security in mind. They can be replicated over and over again, used to create and deploy a number of applications offering standardization, compliance, agility and reliability throughout an organization.

For more detail on how to standardize your organization's architecture in AWS, click here.

Automate Compliance with AWS CloudFormation

AWS CloudFormation is the vehicle that empowers you to achieve compliance for applications throughout your organization. Overall, CloudFormation offers plug-and-play JSON template files that allow you to smoothly and continuously deploy architecture.

Another key piece of the puzzle has to do with stacks. As a refresher, stacks are individual sets of resources that can be configured to meet the compliance needs of your organization, per template. Using a modular approach to architecture you can layer individual stacks that have common configurations for certain applications. Furthermore, you can set and automate the baselines of your architecture, as described above, and deploy them through like applications.

Once all of your stacks have been created for a specific use-case, you can bundle those together into a package that can be replicated and deployed, as needed.

Tips for automating governance in AWS, include the following:

- Use modular development, nest stacks into layers and package them
- Define your compliance parameters in advance, knowing how to use a parameters file
- Implement contingencies that make sense for your organization and dependencies
- Use IAM to keep users from being able to delete important stacks

The key to automating compliance within your organization's instance of AWS is understanding your business needs, allocating the resources within your organization to implement them and having the knowledge and ability to do so with success.

Final Thoughts

In the end, having a good handle on governance can lead to greater profits to the tune of about 20%. For any business, that's no small chunk of change.

Today, as enterprises transition their processes almost entirely to the cloud, new questions of governance arise regarding the relationship between businesses and their cloud providers. When it

comes to AWS, a shared responsibility model reduces operations concerns for end users, but organizations can further reduce risk by implementing MSO teams to do some of the governance heavy lifting.

The good news is that BMC can work with you to be your AWS managed services partner. BMC helps ensure your success with AWS in several ways from migration planning by enabling your DevOps and big data initiatives.

In addition, as it relates to compliance and governance for AWS, BMC Helix Cloud Security (formerly TrueSight Cloud Security) automates security testing and remediation for multi-cloud resources and containers, to manage configurations consistently, securely and with an audit trail. There are several key benefits of the platform including:

- Consistent, secure configuration of the cloud resources which your apps consume, without impeding innovation or velocity
- Multi-cloud security at scale through automation, removing the manpower bottleneck
- Identify and fix compliance violations quickly, efficiently
- Avoid the risks and costs associated with a cloud security breach or compliance violation

For more information on how BMC can meet your compliance and governance needs with AWS, click here.