

**DEFINITIVE CLOUD  
GOVERNANCE GUIDE:  
11 TENETS OF  
CLOUD STRATEGY**



# Table of contents

- Introduction** ----- 3
- What are the challenges?** ----- 4
- 11 tenets of cloud governance strategy** ----- 5
  - 1. Account organization ----- 6
  - 2. Networking ----- 7
  - 3. Budgets and cost management ----- 8
  - 4. Tagging ----- 9
  - 5. Security guardrails ----- 10
  - 6. Compliance enforcement ----- 11
  - 7. Security logging ----- 11
  - 8. Infrastructure automation ----- 12
  - 9. DevOps ----- 13
  - 10. Secrets management ----- 14
  - 11. Configuration management ----- 15





Organizations migrate to the cloud for benefits like elasticity, cost savings, high availability, and improved efficiency. While companies with a smaller number of workloads can instantly realize these benefits post-migration, enterprise-wide cloud migration initiatives take longer and are often riddled with challenges.

These challenges center around the fact that cloud service providers offer their services as building blocks for cloud as only the foundation; not for out-of-the-box production. As organizations seek highly-skilled cloud resources to help them build upon those services, they often face resource constraints and/or skills gaps as limitations to moving forward.

Most organizations adopt a siloed approach to their IT strategy (Dev, Security, Application teams, Networking, IAM and more all acting as separate groups) resulting in a bottleneck a workload owner faces when having to coordinate with each of these teams for their part in migrating to the cloud. Compound these challenges across all workloads in the organization and the barriers faced in an enterprise-wide cloud initiative become significant.

The good news is that a cloud migration strategy leveraging automation can streamline the process. By implementing a cloud governance model up front, organizations can define their cloud policies, protocols, procedures, best practices, governance, security and compliance, budgets, and overall guardrails one time and reuse it many times. Eliminating the chance of human error, automation helps remove bottlenecks in critical processes, and accelerates the enterprise's overall journey to the cloud.



## What are the challenges?

To understand the challenges that keep organizations from realizing the benefits offered by the cloud, it's important to understand two key factors – the cloud offering and the workforce managing the cloud ecosystem.

### Cloud offering

Cloud service providers offer building blocks – not houses. All cloud service providers make it easy for users to launch their services, with most of them requiring little to no human intervention to remain operating effectively and efficiently. But operating under what circumstances? For example, while a developer could deploy something to the cloud in a day, would it meet compliance, security, access, costing, and logging requirements?

### Workforce

There is a serious shortage of skilled workers who can work efficiently within the cloud landscape. This drastically impedes the velocity at which a company can migrate to the cloud.

While most technical practitioners are specialists—who have their own forte and prefer to spend their time and energy working within that realm—a cloud environment favors polyglots. Polyglots are comfortable with a wide range of technologies and tools. They show a willingness to own and deliver tasks that are beyond their core realm of expertise. Their willingness to learn aspects like security, networking, scripting, and operating systems allows them to create an enterprise-grade cloud ecosystem even if they lack experience.

The percentage of polyglots is typically smaller than the number of specialists in the market as well as within enterprises, especially when their primary business is not technology. The dearth of talent combined with the challenges of siloed teams in most enterprises makes the cloud adoption process highly sequential—creating a bottleneck for the adoption and migration process.



There is a serious shortage of skilled workers who can work efficiently within the cloud landscape. This drastically impedes the velocity at which a company can migrate to the cloud.



## 11 tenets of cloud governance strategy

To negate the challenges previously outlined, organizations can invest up front in building an automated governance strategy. By leveraging the tools offered by cloud service providers and third-party players, companies can successfully pave the way for teams to migrate their applications efficiently and securely to the cloud. This can be achieved without causing much disruption to an organization's team and their skillsets.



# 1 Account organization

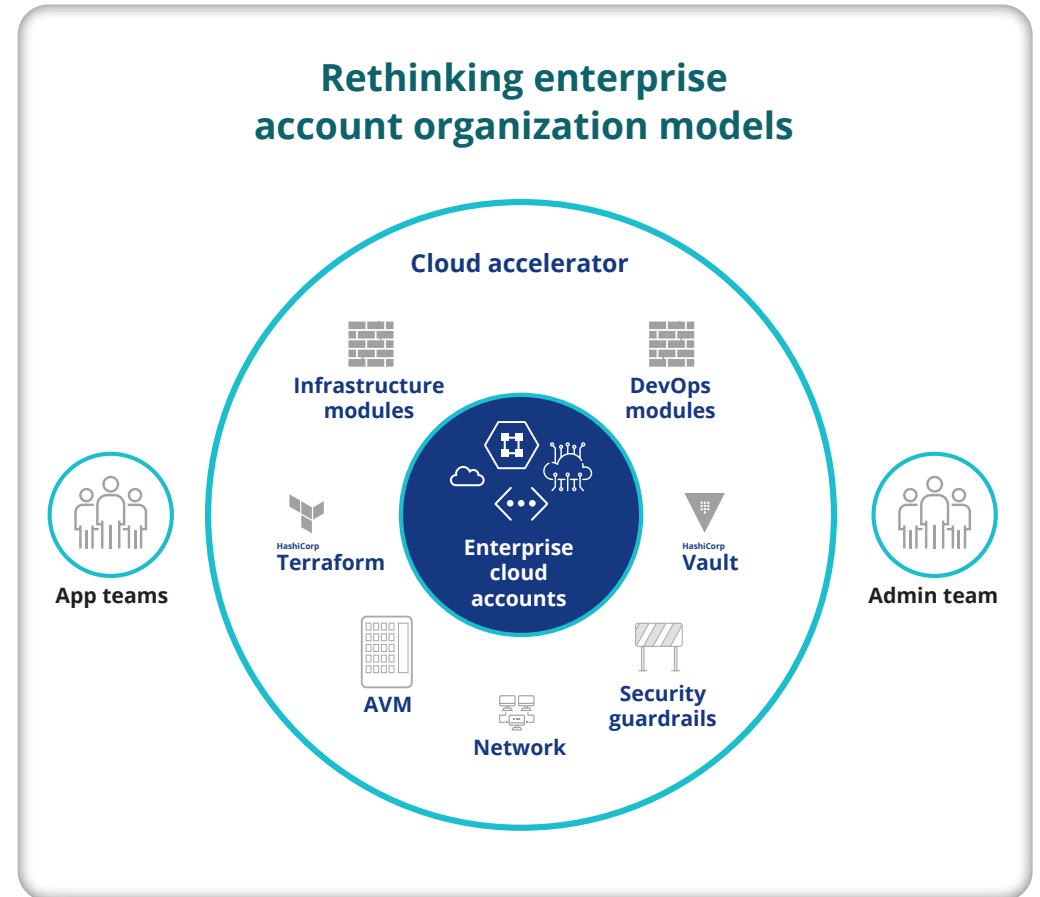
As recently as a few years ago, companies used cloud accounts (subscriptions in Azure and projects in GCP) as multi-tenant containers for all their workloads. Separating production and non-production workloads using regions was the only form of isolation employed. Today, cloud providers have added more robust features to their catalogs to enable isolation. We recommend that customers isolate workloads in Organization Units based on the following:

- > Environment Category (Production, Pre-Production, Non-Production, Sandbox, and Shared Services).
- > Business Units / Cost center – Each business unit gets its own set of the above-mentioned account types.
- > Data Sensitivity – Workloads dealing with sensitive data get their own Organization Unit.

Operating under a well-understood, folder-subfolder model, a well-planned OU structure can help companies achieve the following benefits:

- Security:** Reduce the blast radius.
- Compliance:** Apply compliance and security policies at OU-level which can be propagated to its members.
- Accounting:** Take advantage of the volume benefits while generating OU-specific invoices.

*Setting up the organization is a one-time process and is typically done manually.*



## 2 Networking

A good network design is essential for cloud infrastructure because it offers:

- > Isolation between workloads.
- > Connectivity between private networks.
- > Efficient use of IPs.
- > Protection against unauthorized access to workloads.

Good design takes into account how subnet architecture—the building blocks of a private network—will connect between various enterprise services. Cloud providers like AWS associate subnets to availability zones (distinct locations within an AWS Region that are engineered to be isolated from failures in other Availability Zones). In this case, workloads can be distributed across multiple subnets to achieve high availability during availability zone (AZ) failures. Here are some widely-used subnet architectures:

- > All non-production networks and production networks hosting exclusively intranet sites will not have any public subnets.
- > Each private network will have one or more subnets which have connectivity to other private networks within the organization. This is required when a subset of workloads in each network needs access to a shared service like an enterprise Bitbucket server or Active Directory.
- > Private networks on Sandbox cloud accounts which are meant for developer experiments will not have any routes back to datacenter or other networks.
- > Setting up subnets dedicated to databases, backend applications and front-end applications (and appliances like load balancer) is customary practice. This will allow admins to easily restrict access to those components using firewall rules.

*Transit gateway and network peering are commonly-used approaches to enable connectivity between these private networks.*



Good design takes into account how subnet architecture – the building blocks of a private network – will connect between various enterprise services.







### 3 Budgets and cost management

Adopting an automated approach to setting and enforcing fiscal policy is a fundamental quality of a good cloud governance model. Automation ensures spending is actively-monitored and controlled in close-to-real-time. When budgets are aligned with projects and accounts, automation ensures budgets are maintained in real time, and accounts cannot exceed an approved budget. Here are a few commonly used patterns to enforce budget constraints:

- Organizational Units have budgets associated with them; automatic reporting enables immediate notification as allocations are neared or reached.
- Spending dashboards facilitate forecasting and better budget planning.

Several money-saving measures can be implemented within this cloud framework. A few of them are:

- Controls that prohibit users from creating certain expensive resources.
- Enabling utilization resources from cloud providers.
- Automated shutdowns of non-production workloads during non-business hours.
- Building a repository of a service catalog for commonly used patterns and making it available for application teams



## 4 Tagging

Most organizations know that tagging resources is critical but it is important to have a mechanism to enforce tags.

- > Having controls in place to detect resources without tags that will take remediation action. For example, on AWS, this can be achieved using AWS Config.
- > Building service catalogs/terraform modules which enforce all identified tags out-of-box.



Tagging resources is important for the following reasons.



### Cost Allocation Tags

Allows accurate chargeback.



### Contact Tags

Tags with the contact information of the resource owners will enable the L1 support team to reach out to the right people during issues.



### On/Off Tags

Tags containing schedule information on when to turn on and off can be leveraged automations to turn off non-production workloads during non-business hours.



### Application Tags

Tags with application names are often used by configuration management tools like Ansible and Chef to synchronize changes.



### Data Classification Tags

Tagging workloads based on the sensitivity of the data handled by them makes it easier to enforce compliance and enable automated audits.



### Expiration Tags

This tag can be used to specify dates beyond which the given resource is not required, and automation scripts can pick this date and terminate them after expiry.



Many, if not most, of the security breaches in the past few years have been a result of a cloud loophole. An organization should prepare a list of security guardrails for each resource.



## 5

### Security guardrails

Many, if not most, of the security breaches in the past few years have been a result of a cloud loophole. An organization should prepare a list of security guardrails for each resource. These guardrails are comprised of two types.

- > **Preventive** – Some of the preventive types of guardrails come as part of major cloud provider offerings (AWS Control tower/Landing zone, GCP organization policy constraints). They prohibit anyone from creating resources that do not adhere to security best practices or might be a threat to the organization. (Open security group of EC2/RDS to Public or Creating S3 bucket with Public read/write access).
- > **Detective** – Detective guardrails will identify an illegal resource after it is created. With the use of these guardrails, we can immediately notify the stakeholders and ask the user to delete the resource. Further notifications can go to the automation security team who can also remove the resource. All cloud providers offer most of the commonly used Detective guardrails (AWS Config, GCP security command center) as well as the option to write custom guardrails if required by the organization. A good example of this is using encryption keys to encrypt all the storage volumes.

## 6 Compliance enforcement

In most enterprises, the compliance team often works with the security team to make sure all services used in their organization follow their policies. Healthcare companies need to follow HIPAA compliance. Credit card companies need to follow PCI DSS. Major cloud providers get all these approvals for the respective service and then only organizations can use that service.

Services used to enforce compliance are typically the same as those related to security guardrails. The same approach can be used to restrict access as well as to identify any resources not in compliance.



## 7 Security logging

Auditability in a cloud ecosystem is a fundamental requirement for enterprises. All of the actions on each of the cloud accounts need to be centrally logged. Security and compliance teams can automate notification of any occurrence of an undesired event—allowing quick action to alleviate breaches and threats.

Dashboards and reports on infrastructure vulnerabilities and non-compliances can keep the team apprised and keep their focus on remediating them.



## 8 Infrastructure automation

It is critical that enterprises create a repository of reusable infrastructure libraries that incorporate all the company and industry best practices. Here are the key benefits of this approach:


- > **Reduced complexity** – Provisioning production-grade infrastructure is a complex and time-consuming process and requires specific skills. Finding widely-used cloud services and building or leveraging publicly-available infrastructure libraries eliminates or simplifies the infrastructure provisioning process for application teams.
- > **Reduced errors** – Infrastructure automation greatly reduces the error rate associated with the manual provisioning of servers. Since all the necessary infrastructure gets provisioned automatically, without any human intervention, it reduces the chances (and impact) of error while empowering IT teams to focus on tasks that are mission-critical for the organization.
- > **Reduced time-to-market** – Teams can rely on automated provisioning to get started building products sooner and bring them to the market faster—thus outpacing the competition and meeting customer demands effectively.
- > **Simplified incremental improvements** – The catalog of reusable infrastructure libraries can be constantly updated based on current trends and best practices. The existing infrastructure can be easily retrofitted with the latest changes if they are using an older version of the libraries.
- > **Secure and compliant out-of-box** – These libraries can incorporate security, tagging and other compliance requirements out-of-box.




## 9 DevOps

A DevOps model allows more frequent releases and enables better collaboration between engineers and teams. When migrating to cloud, one of the biggest challenges faced by the DevOps teams is the need to learn new DevOps services offered by the cloud provider and to generate reports like the ones generated in their current setup. Enterprises can make this process less painful by taking the following steps:

- 1 Define the account/project/subscription which is going to host the SCM and the DevOps pipeline for application.
- 2 Setup accesses which allow those pipelines to make deployments to intended target accounts/projects/subscriptions.
- 3 Identify widely-used services to host the workloads and build reusable infrastructure libraries capable of setting up the DevOps pipelines for them.
- 4 Document the KPI and reporting requirements and build automation enabling them when a new application is onboarded.



A DevOps model allows more frequent releases and enables better collaboration between engineers and teams.





## 10 Secrets management

Managing secrets can quickly get out of control when each application team can use its own strategy. All major cloud providers offer their own set of services specifically designed to manage secrets – they can enforce the password policy and rotation and encrypt data at rest and in transit. Encouraging application teams to use such services simplifies management from the governance team standpoint.

Typically, large enterprises tend to have a dedicated solution for secrets management like CyberArk or Hashi Vault. In such cases, it helps if they have automation which creates resources on those solutions and grants access to the application being on-boarded to cloud. This eliminates the need for a dedicated team to work closely with each application team, manually creating vaults/containers to host their secrets and granting access to their members.

## 11 Configuration management

Configuration management tools like Ansible, Chef and Puppet play a significant role in keeping this ecosystem fully automated. When the various operating teams deploy their services via automation, companies can eliminate all human-related bottlenecks impeding the velocity of cloud migration. Here are some common configuration management use cases:

- > Network teams manage the routing table to allow connections between networks.
- > Firewall teams manage the WAF/Firewall rule centrally.
- > Operating systems teams update and patch servers.
- > DBA teams apply their hardening/audit scripts to all the databases.
- > Specialty teams are in charge of installing, patching, and managing application servers like WebLogic, WebSphere, and WordPress.

Identifying all the configuration management use cases, forming small teams that can build reusable libraries for all those use cases, and creating documents for application teams to consume will save a lot of time and money during application migration.

As organizations look to migrate to the cloud for elasticity, cost savings, high availability, and improved efficiency, they will face challenges to do so quickly. By building and leveraging a cloud migration framework, IT departments can mitigate all those challenges to accelerate the enterprise journey to a secure, compliant and operationally-efficient cloud environment.



By building and leveraging a cloud migration framework, IT departments can mitigate challenges to accelerate the enterprise journey to a secure, compliant and operationally efficient cloud environment.



# HGS DIGITAL

With over 250 digital successes and stellar client satisfaction ratings, HGS Digital creates frictionless customer experiences that solve complex business problems and improve people's lives.

We work with leading brands across the world to improve their customer engagement, optimize their operations, reduce costs, and increase revenue. As a technology-agnostic consultant—with partners ranging from Amazon, Salesforce, Google, IBM, Microsoft, and more—we are well-equipped to help you select and successfully implement the right tools for your specific needs.



[www.hgsdigital.com](http://www.hgsdigital.com)



[sales@hgsdigital.com](mailto:sales@hgsdigital.com)

