Enabling enterprise governance in Azure

At Microsoft Core Services and Engineering (CSEO), we’ve used Azure governance to create a solution that enables enterprise-scale governance and compliance enforcement for our entire Azure environment. By using Azure governance, we can enable governance across multiple subscriptions, and also create management and enforcement policies that fit our enterprise model, to make our Azure environment more robust, secure, efficient, and effective.

Adopting a cloud-centric architecture at Microsoft

Over the past few years, Microsoft has been undergoing a mass migration. We’ve moved more than 95 percent of our technology workloads from on-premises servers in datacenters to Microsoft Azure and cloud-based solutions. Migration to the cloud has changed the way CSEO operates, and it’s helping Microsoft to enable a larger digital transformation that affects the entire organization.

Examining the Azure environment

Azure is now the single largest host of our IT infrastructure. The rhythm of our business relies on the Azure platform and the large variety of Azure services that we use to enable our enterprise. The CSEO landscape at Microsoft looks something like this:

- 124,000 employees
- 587 locations
- 700 Azure subscriptions
- 1,600 Azure-based applications
- 11,000 Azure infrastructure as a service (IaaS) virtual machines
- 384,000 managed devices

Enabling digital transformation

Our cloud-centric architecture is one of the primary CSEO investments supporting digital transformation at Microsoft. Our transformation is at the core of our growth as a business, and it’s affecting our entire organization. Cloud-centric architecture in Azure supports our continued growth in several ways, by:

- Providing an agile and reliable platform on which we can build scalable and flexible solutions.
- Enabling broad access to solutions for our employees and customers so that they can work wherever and whenever it best suits them.
- Moving our fiscal model toward a predictable and cyclical operational expenses model.
- Providing modular and open-source tools that help our engineers rapidly build and deploy business-critical solutions.

By embracing digital transformation and the adoption of a cloud-centric architecture, our business is now deeply rooted in the cloud, and we depend on Azure to handle almost all our business platforms and tools.
Aligning with a DevOps culture

As part of our digital transformation, we have fundamentally changed the way that we deliver our products and services and how we develop our internal solutions. We’ve fully embraced modern engineering principles, including the Agile methodology and a DevOps approach to develop and operate our solutions and services.

DevOps redefines the development and operations cycles for solution development, combining them both into a more flexible and solution-focused approach. The adoption of DevOps within CSEO directly affects how we manage and build our Azure environment. DevOps thrives with increased autonomy, and it is designed to empower teams to measure, deliver, fail, learn, and improve internally to generate business-driven outcomes. With increased autonomy, however, comes reduced control for centralized infrastructure management. This centralized management that was core to the on-premises security model no longer meets the requirements of a more autonomous, agile, and fluid cloud-based environment built and operated in the DevOps model.

Operationalizing the cloud

Our distributed and DevOps-focused Azure environment requires a two-tiered approach to everything that we develop and operate. Our DevOps teams are given autonomy over the main areas of their solution, including implementation, core monitoring, and alerting. If an issue arises in the operations of any application at CSEO, the application’s developers—who are also the operations team—are responsible for resolving the issue. In practice, our DevOps approach divides responsibilities into two team categories:

- **Centralized enterprise team.** This group is responsible for the overall health of our cloud environment and for ensuring that the critical aspects of the entire environment, such as business continuity and legal compliance, are properly addressed.
- **DevOps teams.** These groups develop and operate our solutions. They design the business objectives, create the code, implement the solution, and ensure that it operates properly within its context. There are thousands of DevOps teams across Microsoft who manage their solutions and operate the core functionality of our enterprise.

This model drives the functionality of our Azure infrastructure and directly informs the way that we monitor and govern that infrastructure.

Adapting to a changing security model

With the majority of our corporate data and infrastructure hosted in the cloud and our practices becoming more and more decentralized, we recognized the need to assess our security models—initially developed for the traditional, on-premises datacenter—and examine the changes necessary to provide a robust and trustworthy environment in the cloud-based DevOps environment. The cloud environment presents several key differences from the traditional datacenter:

- **Users have open access to cloud infrastructure, from any network or device.** The network is no longer a hard and static security boundary. The cloud is internet connected and broadly available.
- **Sharing models are unrestricted.** In the cloud, data-sharing activities are typically within the control of the data owner, who can decide when and with whom they want to share their data.
- **The cloud uses an open app and access ecosystem.** Cloud resources are accessed by using easily downloadable tools and apps, which expands access to any users given the appropriate permission.
- **There is limited visibility into cloud infrastructure.** Cloud resources are distributed by nature and are owner controlled. This means that visibility into multiple environments managed by different people can be cumbersome and difficult to achieve.

Enabling the compliant cloud with Azure governance

At CSEO, we wanted to apply the Microsoft enterprise context to our entire cloud-hosted environment to enable our engineers to leverage Azure services in a secure environment by using a model that enabled a DevOps approach to our infrastructure. To apply the enterprise context, we wanted to design, develop, and implement an engineering
solution in this new model that enabled CSEO to efficiently and automatically deploy enterprise-scale cloud configuration standards.

### Setting goals for the compliant cloud

The Azure governance model and the differences it brought led us to establish a set of goals that would guide us in applying a new security model to our new cloud-based enterprise. The goals included:

- **Enable safe self-provisioning.** We wanted to create a simple way to support self-provisioning but also ensure governance throughout the process. Self-provisioning allows for user-directed resource creation. User-directed methods remove our central management teams from the creation process, which means that they can’t ensure that a resource is created within governance parameters.

- **Create self-governing application environments.** We wanted to have methods in place to ensure that governance would be applied to an environment and maintained throughout the lifecycle of the application, or until governance parameters changed.

- **Establish a multitiered model for governance.** We wanted to view and enforce compliance-related governance at the same levels that we operated our business. Each business group needed to have autonomy over their environment, but we also needed to create enterprise-wide visibility and control over important areas that affected the entire enterprise.

- **Embed security into our DevOps processes.** We were using some tools as a good starting point for DevOps engineering processes but wanted to carry the methods into the Azure environment to enable enforcement and consistency across our entire environment.

### Examining Azure governance

We adopted Azure governance as the foundation of our compliant cloud solution. Azure governance is a collection of concepts and services that are designed to enable management of Azure resources at scale. These services provide the ability to organize and structure subscriptions in a logical way, to create and deploy reusable packages of resources, and to define, audit, and remediate resources.

Azure governance provided the key components that we needed to apply our corporate context and create an enterprise scale governance solution for our CSEO Azure environment. These include management groups, policies, initiatives, and telemetry.

### Azure Management Groups

Azure Management Groups provide a level of scope above subscriptions. With the Management Groups feature, we can organize subscriptions and apply governance conditions to the management groups and the subscriptions contained within those groups. All subscriptions within a management group automatically inherit the conditions applied to the management group. Management groups give us enterprise-level management across all our subscriptions.

### Azure Policy

Azure Policy helps us manage and maintain compliance with policy definitions that enforce rules and effects for our Azure resources. Azure Policy provides the majority of compliance functionality within our Azure governance solution by handling tasks such as:

- Assigning a policy to audit or enforce a condition for resources within the portfolio.
- Creating and assigning an initiative definition to assign multiple policies across a portfolio of resources.
- Providing granular compliance information about the resources evaluated against specified conditions.
- Resolving noncompliant configuration or denying the creation of resources that do not meet the conditions.
Policies consist of a definition that contains the enforcement rule and an assignment that determines the scope of Azure resources that the policy affects. **Initiatives**
An initiative is a collection of policy definitions that are targeted toward a singular overarching goal. Initiative definitions simplify managing and assigning policy definitions by grouping a set of policies as one single item. For example, we’re using initiatives to create two focus areas within our Azure governance implementation: one initiative for enforcing a desired state for security across the enterprise, and another initiative for examining infrastructure and platform state across all our Azure infrastructure.

**Adopting Azure governance**

Azure governance gave us a toolset that would enable us to create a solution that met our primary goals and satisfied our needs for enterprise-scale compliance. We set several high-level implementation goals for our Azure governance solution to guide our development:

- Partner with Microsoft Security and Azure experts to define cloud configuration standards and compliance targets across our entire internal Azure environment.
- Leverage Azure-native capabilities to implement a solution and governance framework to deploy and enforce cloud configurations at an enterprise scale.
- Enable efficient compliance management and reporting at scale for the enterprise.

**Democratizing our governance approach**

In continuing with our DevOps approach to Azure, we planned our Azure governance implementation around our decentralized business model. In that model, accountability for the Azure environment is bifurcated, and CSEO provides frameworks that enabled autonomy, enforced enterprise-level standards, and provided guidance and support. Our model was structured as follows:

- Our Cloud Center of Excellence team within CSEO provides capabilities that maintain Security monitoring, infrastructure monitoring, change management, patch-compliance governance, data collection for inventory, and cost-management governance. The Cloud Center of Excellence team is responsible for the following implementation areas:
  - Hosting environment
  - Self-service automation and toolkits
  - Major-incident support
  - Cloud standards and policy
  - Consulting and guidance
  - Cloud fabric management and optimization
  - Problem management support

- Engineering teams for each Azure solution are empowered to enable improved autonomy and flexibility when creating infrastructure, including patch deployment, change configuration tracking, solution monitoring, performance analytics, and security monitoring. Our engineers are responsible for the following activities:
  - Author infrastructure by planning, forecasting, and provisioning with automation.
  - Leverage design patterns, standard templates, and management packs.
  - Leverage assisted crisis management.
  - Programmatically consume and execute against standards and policy.
  - Leverage infrastructure engineering expertise for complex scenarios.
  - Automate environment management.
  - Customize alerting and diagnostics.
Enabling automated guidance with policy enforcement

We allowed our engineering teams autonomy in implementing their Azure solutions. At the same time, it was important to ensure that our engineering teams had established guidelines within that autonomy to prevent mistakes and misconfigurations that put CSEO at risk in areas such as security or regulatory compliance. Azure governance enabled us to create a set of boundaries for our engineering teams that ensure that they adhere to the best practices for our Azure environment. Before Azure governance, the manual deployment of resources, manual enforcement of policies, and manual remediation of issues increased risk for human error or misconfiguration.

Azure governance gives us a way to implement policies that provide automated “guardrails” that keep our engineers within our Azure standards. This assures both CSEO and the engineering teams that they are always developing to the appropriate standard. We’ve used Azure governance to establish:

- Automated deployment, enforcement, and remediation of cloud configuration and security requirements through Azure’s native capabilities.
- Compliance by default through specific policy effects.
- Native compliance reporting per subscription and centralized reporting for an organization’s portfolio.
- Azure-first implementation that influences product direction.
- Collaboration and alignment between Microsoft security groups for tenant-wide policy and configuration requirements.

Building an effective framework in Azure governance

We use Azure Management Groups to create a logical hierarchy within the Azure governance environment. Azure Management groups can be nested, so we use the nesting behavior to replicate the relevant business and engineering structure for the groups and organizations that support each subscription.

Creating a logical structure and hierarchy

We maintain a Cloud Steering Committee to oversee primary cloud operations, and the committee serves a vital role in making decisions on the deployment of policies across CSEO. The Cloud Steering Committee includes representatives from various organizations within Microsoft such as Security, LOB Engineering, Azure subject-matter experts (SMEs) by service or technology stack, and business leaders. These individuals have a broad range of expertise and are expected to review technical, security, and business implications associated with deploying mandatory policies across CSEO.

We manage an automated service that replicates our organizational structure from our service management tool into a hierarchy of Azure management groups. Our organizational groups have significantly different needs and requirements for policy application, and replicating our organizational structure allows us to provide each group with autonomy over their portion of the environment. Logical structure differs from organization to organization. For more information, consult the governance section of the Microsoft Cloud Adoption Framework for Azure. Our hierarchy includes multiple levels, and contains three primary level definitions:

- **Level 0: Tenant.** Level 0 represents the top of the Azure hierarchy and the broadest scope. Deploying a policy to level 0 requires security leadership review and approval.
- **Level 1: Managed scope.** Level 1 represents our larger divisions. Deploying a policy at this level requires review and approval from our Cloud Steering Committee.
- **Level 2+: Nonmanaged scope.** Any policy applications below level 2 are at the discretion of the organizational and service groups associated with the subscriptions affected and are not subject to Cloud Steering Committee approval.
Deploying policy
Management Groups enable us to logically group our subscriptions and deploy Azure policies at scale across all 700 subscriptions that CSEO manages. Policies are authored by engineers and checked into Azure DevOps. When the engineers are satisfied that the policy is ready, they submit a pull request that is reviewed by the Cloud Steering Committee. Once approved, the build and release processes are launched in Azure DevOps where the deployment occurs. The automated deployment uses policy as code for configurable and easily re-deployable policies.

Figure 1. The cloud governance hierarchy

Figure 2. An overview of the governed cloud with Azure governance
Best practices

- **Enable automation wherever possible.** Although automated processes take time to develop, the time-savings and consistency benefits of automation usually outweigh the effort required to automate tasks.

- **Consider how you use policy enforcement and inheritance.** You can use policies as hard controls that specifically disallow resource deployment. These policies will ensure that noncompliant resources are not deployed, but they can stop progress and delay development. Use these policies only for mandatory requirements. You should also leverage inheritance and apply broadly applied or security-related policies as high in the hierarchy as possible.

- **Map Azure Management Group hierarchy to a logical structure.** Azure Management Groups provide the ability to manage the Azure portfolio at scale. Ensuring that Management Groups map accurately to your logical structure, make it easier to deploy policy. Logical structure could be based on environment, business structure, or other compositions specific to your organization.

- **Leverage Azure Management Groups beyond policy application.** Azure Management Groups enable you to perform additional management tasks across subscriptions. You can use management groups for other enterprise-management scenarios, including cost management, reporting, and solution management.

- **Enable robust end-to-end monitoring and alerting.** Management Group access can provide wide-ranging permissions within Azure, so how your access model is configured is critical. It might be necessary to leverage Privileged Identity Management (PIM) as part of a comprehensive strategy. PIM allows administrators to request just-in-time access. We’ve been using a two-key system for administrative access that ensures that no single individual can make critical changes on their own. It’s also important to monitor Management Group events such as creation, deletion, and modification along with permissions changes. Most of this information is written into the standard Azure Activity Log.

Moving forward

Now that we have defined a democratized governance framework that works in a DevOps culture, using native tools to build a scalable solution and a strong partnership with the Azure governance team, we are positioned to enable Cloud Governance to manage CSEO’s Azure implementation at enterprise scale. We’re working toward a more comprehensive Azure governance solution, including explicitly enforced policies and comprehensive compliance management. We’re also working on automated remediation capabilities for noncompliant resources. Our implementation approach is divided into four phases:

- Evaluation of the Azure Services that will be used to build the enterprise solution.
- Secure implementation of Management Groups.
- Deployment of audit policies to enable the transition to compliance management natively in Azure.
- Deployment of enforcement policies to enable the transition to compliance by default.

Conclusion

Azure governance has enabled CSEO to create an Azure-native, enterprise-scale governance solution that will provide decentralized management of our Azure environment and its governance needs. With Azure governance, our environment is more compliant with our organizational policies and, as a result, more efficient, robust, and effective.

For more information

Microsoft IT Showcase

microsoft.com/itshowcase
Azure governance at Microsoft
https://azure.microsoft.com/solutions/governance/
https://azure.microsoft.com/services/azure-policy/
https://azure.microsoft.com/features/management-groups/

© 2019 Microsoft Corporation. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.