AHEAD®

An Introduction to AHEAD's

Azure Governance Framework

If your business is like many other organizations that are in the process of enabling a Microsoft Azure public cloud platform, then you might be struggling with the guardrails needed to secure and manage cost, while at the same time enabling flexibility for the teams consuming cloud services.

While the Azure platform is already very secure, it also allows a great deal of flexibility in configuration. In order to avoid accidentally creating security holes and out-of-control spend, a Governance Framework is required. We created the AHEAD Azure Governance framework to allow enterprises to develop and maintain a fully optimized, and secure environment. The resulting framework will be tailored to your organization's specific business and compliance needs, as every enterprise is different. This guide will introduce you to the components of this necessary Azure Foundational Governance Design.

Public Cloud Benefits

You're probably already aware of the many benefits of moving to the public cloud, such as:

- Reduced overhead from internally managed computing resources
- Increased ability to meet peak demands
- Reduced hardware costs
- Improved business agility in an ever-evolving competitive market

Why Do You Need a Governance Framework?

Because businesses are already operating within frameworks, your organization will need to figure out how to continue to leverage that framework within Azure. When paired with governance and security measures established and maintained via a proven governance model, the benefits of public cloud can be fully realized. The need to establish this model is amplified for organizations with sensitive data, such as healthcare and financial companies.

The objectives of the governance model are to:

- Establish standards
- Define policies
- Implement guardrails
- Improve manageability and operations
- Allow for flexibility & autonomy
- Ensure auditing of the environment

It's imperative that your business find a way to take your existing governance policies and frameworks and optimize them for Azure. This modification is really a decision-making process, as Azure Governance depends on what's already happening within your organization.

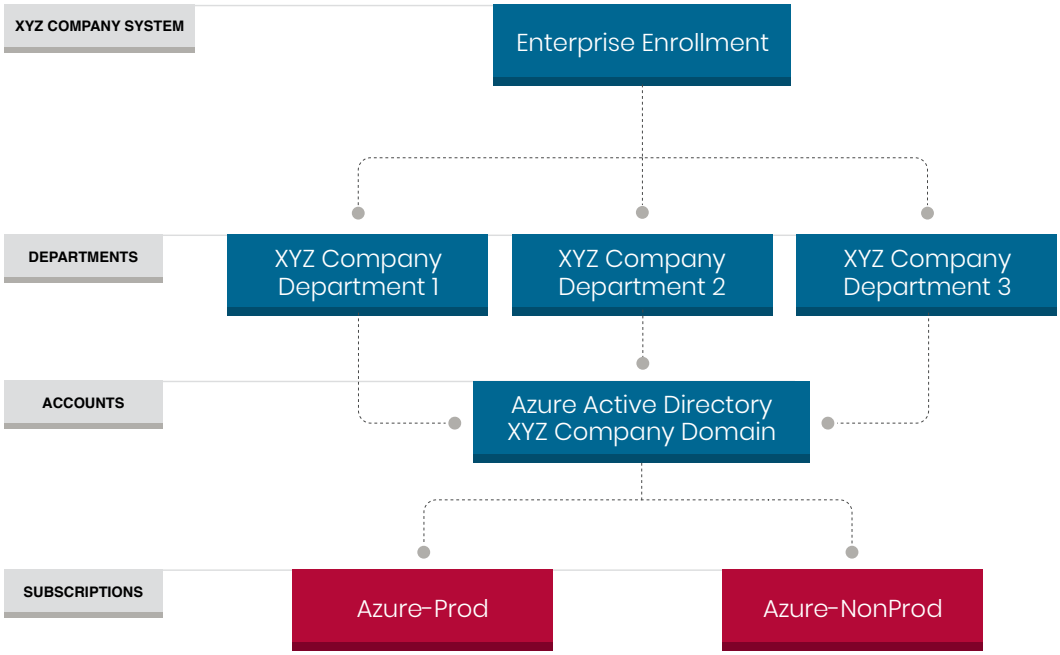
Foundational Governance Model

The Governance Model is based on foundational components as shown in this figure:

Below, we define each of these components as they relate to an organization's overall framework.

Accounts and Subscriptions

Azure services are provided through multiple data centers across geographically diverse global locations. Each client manages their own infrastructure through one or more Azure subscriptions.



As your Azure environment grows, you will need to assess when a new subscription should be created versus creating new resources in an existing subscription

Resource Groups

A resource group is a logical collection of resources within a subscription that contain a common lifecycle or that share some common traits. Proper and consistent use of resource groups is critical to leveraging Azure subscriptions effectively.

Resource Group Design

There are two primary approaches to resource group design:

- Resource groups that encompass all resources and core infrastructure components for an application deployment.
- Centralized resource groups for core components.

In order to determine the best approach for your organization's resource group design, it's necessary to first perform a deeper dive into your environment.

Naming Standards

Naming standards facilitate the identification of resources in the portal, on an invoice, and within scripts. A naming standard must be defined prior to deploying cloud resources.

Tagging Standards

Tagging is the process of adding sets of key-value pairs to an object in order to assign additional metadata to those objects. You'll need to determine best methods and practices to effectively use resource tagging in your organization's environment.

Resource Locks

Azure Resource Locks are mechanisms for locking down resources to ensure protection so that those resources cannot be deleted by just anyone. Administrators spend a lot of time setting up resources in the Azure portal, but by simply modifying options in Azure, users will be "locked out" of the option to delete resources. This also allows for an option to view the resource but not update or delete it.

Resource Placement Policies

Oftentimes you will encounter instances where you will need to implement specific placement policies. For instance, if an organization has restrictions on certain geographies, you can restrict the selection of defined locations in Azure.

Role-Based Access Controls

Azure Role-Based Access Controls (RBAC) can be used to assign permissions to users, groups, and applications at a certain scope.

If your organization does not enforce data access control by leveraging RBAC, you may be granting higher data access privileges than necessary to certain users, making you more vulnerable to data compromise.

Azure Policy Automation

Azure policies provide the ability to govern an Azure environment. Policies can be enforced through automation to ensure data sovereignty by restricting, enforcing and auditing certain actions.

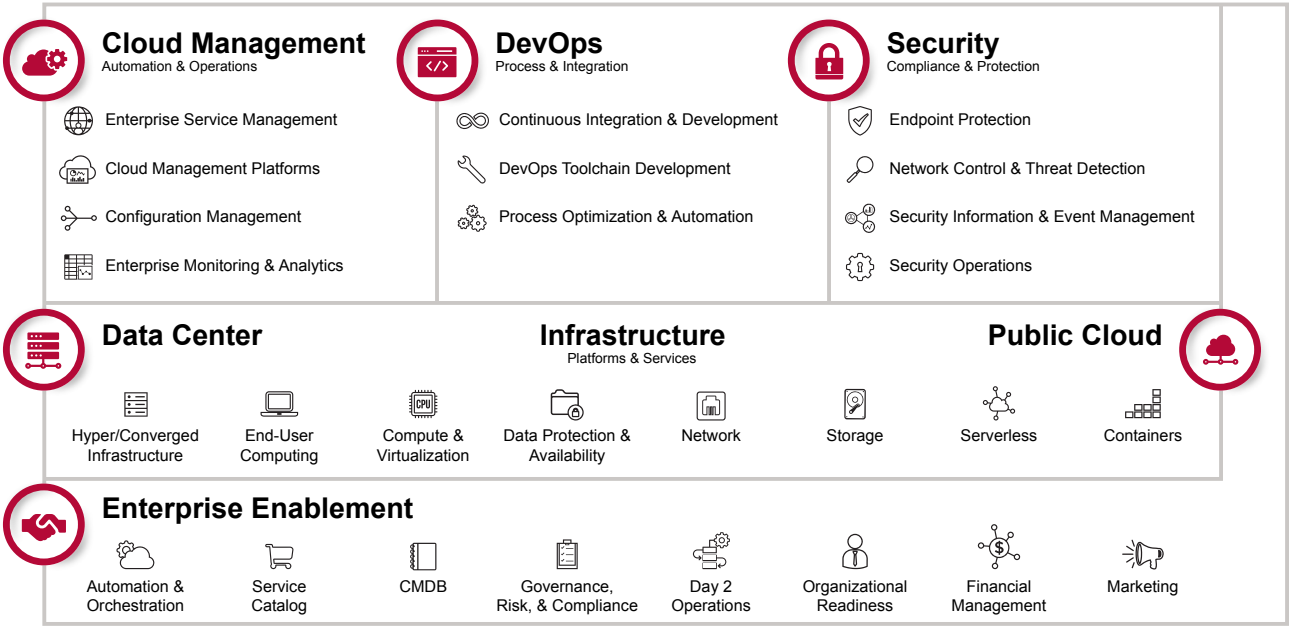
Cost Reporting

Another benefit of the Azure Governance Framework is the ability effectively report on costs based on business departments, specific applications, or accounting units. Your business can utilize Azure's cost analysis features to understand its Azure spend across the organization and generate reports that will be used to distribute to internal accounting units or departments for Azure-related costs. Azure subscription billing information is contained within the Azure portal for easy access and reporting. This functionality allows your organization to view cost data on demand to make decisions in real time.

Auditing

The Azure platform has various auditing options to ensure you're staying within the bounds of your company's compliance frameworks. Logs are used in Azure to collect data connected with your policies and keep you aligned with compliance.

AHEAD Enterprise Cloud Delivery Framework®



AHEAD's experts introduce a concept of this industry-standard Azure Governance Framework in providing established methods to meet security controls, enable automation and DevOps, simplify compliance and audit activities, and build an enterprise approach to next-generation security and governance in the public cloud.

After deploying the Governance Model design that best fits your business, your organization will be strategically positioned to build future cloud-native service offerings against industry security standards and controls.

As shown in AHEAD's Enterprise Cloud Delivery Framework (ECDF) above, governance is just one part of a successful, scalable cloud environment. Interested in learning more about how AHEAD can help ease the burden of the Azure Governance Framework decision process to begin optimizing your organization's environment? Contact us here for more information.

About AHEAD

AHEAD transforms how and where enterprises run applications and infrastructure. From strategic consulting to implementation and managed services, AHEAD creates tailored solutions at all stages of the enterprise cloud journey.

Headquartered in Chicago, AHEAD maintains offices in Michigan, Minnesota, North Carolina, Ohio, and Wisconsin.

AHEAD
401 Michigan Ave.
#3400
Chicago, IL 60611
(312) 924-4492
www.thinkahead.com

In partnership with: Microsoft Azure