After the final task in the preceding list is completed, the VM and supported workload are considered released. The final phase or discipline of migration is now finished for that workload.

Next unit: Knowledge check

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

Knowledge check

3 minutes

Choose the best response for each question, then select **Check your answers**.

Check your knowledge

1. Validating traffic patterns and routing for user traffic is what kind of technical validation?

- ○ User route testing

  ✔ **Having the correct user route testing in place helps ensure that the network is performing as expected.**

- ◉ Network isolation testing

  ✘ **Network isolation testing should be in place to test that the network has proper isolation and no unexpected network vulnerabilities.**

- ○ Dependency testing
- ○ Business continuity and disaster recovery (BCDR) testing

2. What should the phase of assessing workloads in a migration project focus on?

- ○ Form a team of Azure experts
- ○ Gather information about cloud compatibility and dependencies between servers and assets

  ✔ **This phase of the migration project should be focused on information gathering that can help your organization understand the migration path for each workload or asset.**

- ◉ Test and release production traffic to the migrated workloads

  ✘ **The release of production traffic to workloads in the cloud should happen after proper planning and migration.**

- ○ Plan out the migration sprint phases

3. An organization's migration project has stalled because the team hasn't set the correct expectations with its executive-level team. What kind of blocker is this an example of?

- ○ Environmental blocker
- ○ Operations blocker
- ◉ Technical blocker

  ✗ **An example of a technical blocker would be a workload that's not suitable for migration to the cloud.**

- ○ Strategy blocker

  ✓ **Setting the correct expectations across your organization for factors like time frame and budget requirements is about strategy. In a migration project, avoiding strategy blockers can help prevent confusion and delays.**

Next unit: Summary

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Introduction

2 minutes

The Govern methodology of the Cloud Adoption Framework for Azure can help your organization address tangible risks as you adopt the cloud.

Any technical change introduces risk to your environment. Cloud-native tools in Azure help you mitigate risks and adopt the cloud with confidence.

This module demonstrates how to evaluate and respond to risks while implementing guardrails to help keep you safe as you adopt the cloud.

Learning objectives

In this module, you'll:

- Establish processes to properly govern cloud adoption
- Classify tangible risks based on the reference cloud-adoption plan
- Integrate corporate policies to mitigate tangible risks
- List implementation strategies to mitigate risks
- Demonstrate Azure Policy additions that implement risk-mitigation strategies
- Prioritize future governance investments

Prerequisites

- Foundational understanding of IT governance processes
- An understanding of your organization's governance requirements and how they affect your cloud-adoption plan

Next unit: Customer narrative

Continue

100 XP

Customer narrative

10 minutes

In earlier Microsoft Learn modules for the Cloud Adoption Framework, we shared the narrative of Tailwind Traders. The company's central operations and infrastructure teams have successfully migrated some workloads to the cloud, but they face unanswered questions and unexpected concerns as they prepare for production release.

Tailwind Traders' balancing act

Like most businesses, Tailwind Traders is attempting to balance two competing business drivers: digital transformation and risk mitigation.

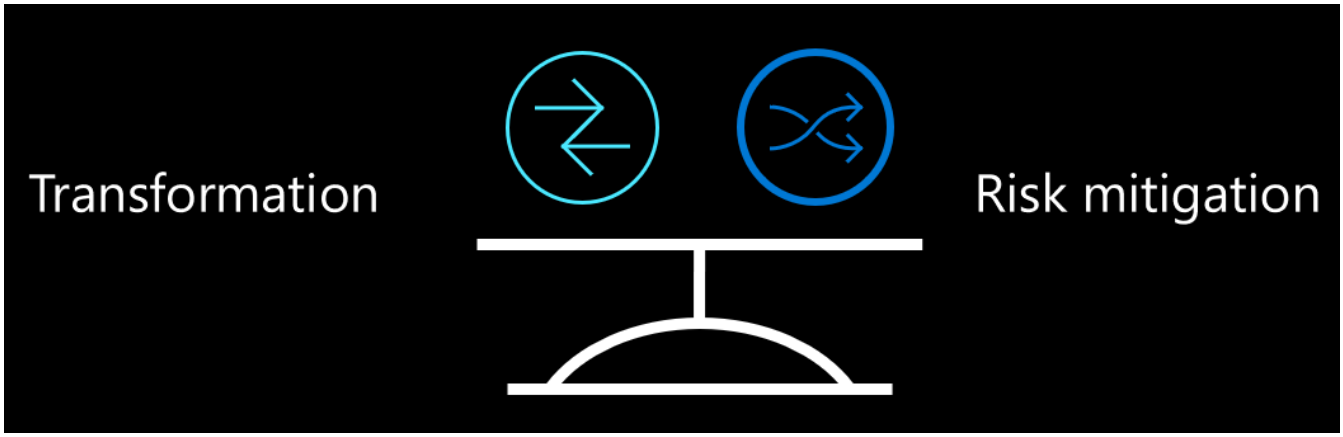


Figure 1: Finding the balance between transformation and risk mitigation.

In the Getting Started module, we shared a few objectives that Tailwind Traders included in its cloud-adoption plan. Most relevant to this module is its effort to migrate out of two leased datacenters in the next 24 months. The datacenters host a large portfolio of production workloads that support in-store and e-commerce operations. One of the datacenters also hosts dev/test environments and other preproduction innovations from the retail innovation team.

Tailwind's effort is driving digital transformation and pushing the boundaries of what the business can do in the cloud. It has migrated low-risk workloads to the cloud. Tailwind also has begun to use cloud-native technologies to innovate and create new solutions that couldn't be delivered on-premises. The value of the cloud is proving out. As Tailwind's adoption plans progress, the need for balance becomes more apparent.

Governance needs

To balance digital transformation efforts, the central operations and infrastructure team needs to find a way to meet the following basic governance needs:

- Maintain compliance
- Create better cost visibility and control
- Apply security posture consistently
- Remain agile to support scale and transformation

Before Tailwind Traders adopted the cloud, governance was delivered by a series of manual processes of review, acceptance, and change control. The employees, processes, and tools that delivered governance functions in the on-premises environment aren't scaling to consistently govern cloud deployments.

Blocked by current policies

The current policy at Tailwind Traders states that "Customer and financial data can only be hosted in a specific network segment of the *existing datacenters*, referred to as protected assets." The policy is problematic, as the business plans its move from primarily using on-premises datacenters to cloud datacenters.

The CIO is working to change the policy, but the central operations and infrastructure team must apply the following controls before the CIO is comfortable approving policy changes:

- Control costs to deliver on the promised savings as adoption scales
- Adhere to security and third-party compliance requirements
- Configure asset management to prepare all workloads to be ready for operations management
- Apply and meet identity and access management requirements
- Follow a path to ensure that all these controls are consistently applied to all workloads while acknowledging the scale and learning curve challenges across the technology teams

Demonstrating that these controls are in place will give the CIO confidence that the team is ready to migrate more complex, higher-risk workloads to the cloud. It also will provide the governance balance that's required.

Unfortunately, the "existing datacenters" governance requirement was discovered only as the team prepared to deploy its first mission-critical workload to production. The policy has frozen the effort to migrate the company's current datacenters. More foresight would have helped the team address this policy sooner as they moved lower-risk workloads to production.

The retail innovation team currently isn't affected by the governance policy, and it has been delivering new innovations in the cloud faster than expected. However, the same challenges will soon block the following teams and efforts:

- The application development teams are working in a dev/test capacity to learn about cloud-native capabilities
- The business intelligence team is experimenting with big data in the cloud and curing data on new platforms

The remaining units in this module will demonstrate the Govern methodology's approach to meeting Tailwind Traders' governance needs, preferably in parallel to cloud-adoption efforts to avoid unexpected project interruptions.

Next unit: Govern methodology

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

Govern methodology

10 minutes

Implementing proper cloud governance requires proper business policy, protective guardrails, and skilled people taking a consistent, disciplined approach to governance.

Build governance maturity

This unit explains the four-step process in the Cloud Adoption Framework to build a mature cloud governance solution:

1. **Methodology**: Understand the underlying methodology
2. **Governance benchmark**: Assess your current-state and future-state needs
3. **Governance foundation**: Establish your governance foundation by using a set of governance tools
4. **Mature governance disciplines**: Iteratively add governance controls to address risks

These steps will get you started using the Govern methodology in the cloud. They also will set you on a path to mature each governance discipline as your cloud adoption plan progresses.

Govern methodology

The Govern methodology provides a structured approach to building the governance maturity that's required for confidence in cloud adoption.

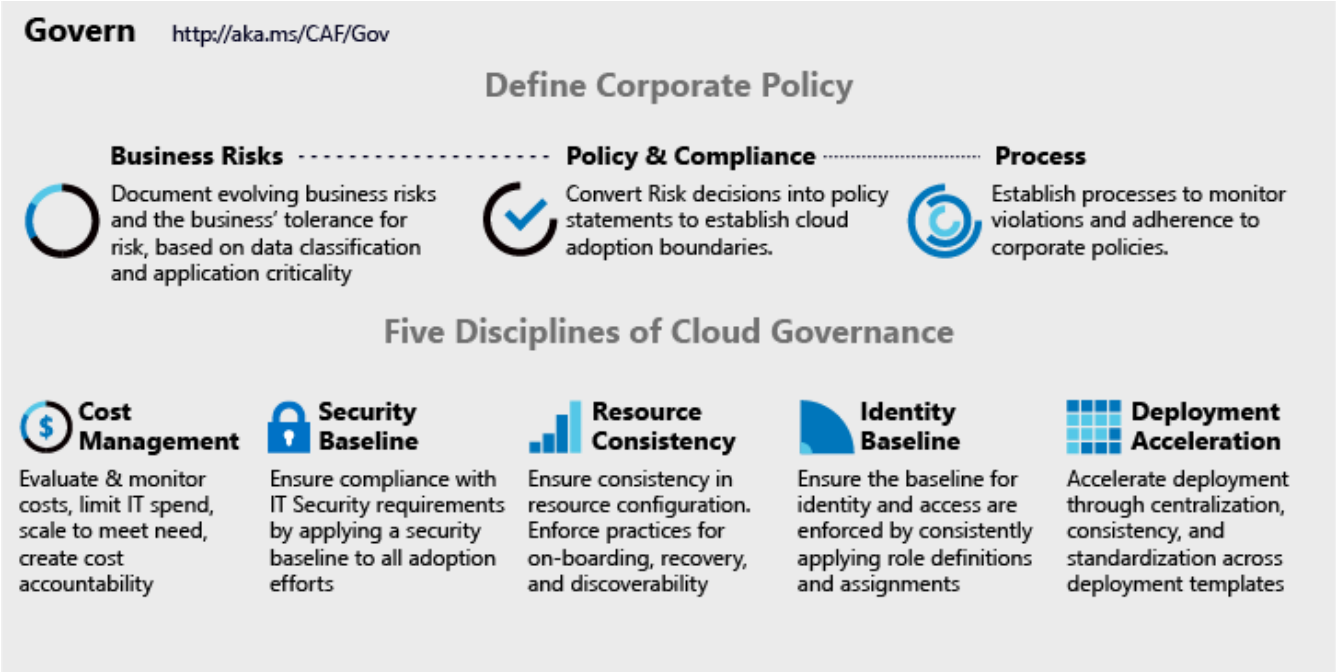


Figure 1: The Govern methodology: define corporate policy and the five disciplines of cloud governance.

Corporate policy

Governance is a big topic, and it might be intimidating at first. Governance seeks to establish the proper scope of corporate actions by mitigating tangible risks through corporate policy.

Corporate policies drive cloud governance. Proper corporate policy consists of three components:

- **Business risk**: Identify and understand tangible corporate risks and the organization's tolerance for risk
- **Policy and compliance**: Convert risks into clear policy statements that support compliance requirements without defining specific technical dependencies
- **Process**: Establish processes to monitor violations and ensure adherence to policy statements

A focus on these components helps develop clear and actionable corporate policies. In the next unit, you'll see how to develop a proper corporate policy.

Governance disciplines

Governance disciplines support corporate policies through a mixture of tools and human processes. Each of the following disciplines protects the organization from specific, defined potential pitfalls:

- **Cost Management discipline**: Optimize costs across a broad portfolio of workloads through the application of budgets, reports, and automated enforcement
- **Security Baseline discipline**: Apply well-defined security requirements to all supported environments and underlying workloads
- **Resource Consistency discipline**: Manage resource configuration at scale to ensure that all deployed assets are discoverable, recoverable, and onboarded into operation management processes
- **Identity Baseline discipline**: Ensure proper authentication and access by applying roles and assignments to each environment
- **Deployment Acceleration discipline**: Standardize and centralize deployment templates to ensure consistency across all environments and workloads

Each discipline accelerates the application of corporate policies and ensures consistent governance. Later in this module, we'll investigate actionable implementation for each discipline.

Governance benchmark tool

The Cloud Adoption Framework provides a governance benchmark tool to help you identify gaps in the governance disciplines and corporate policy in your organization.

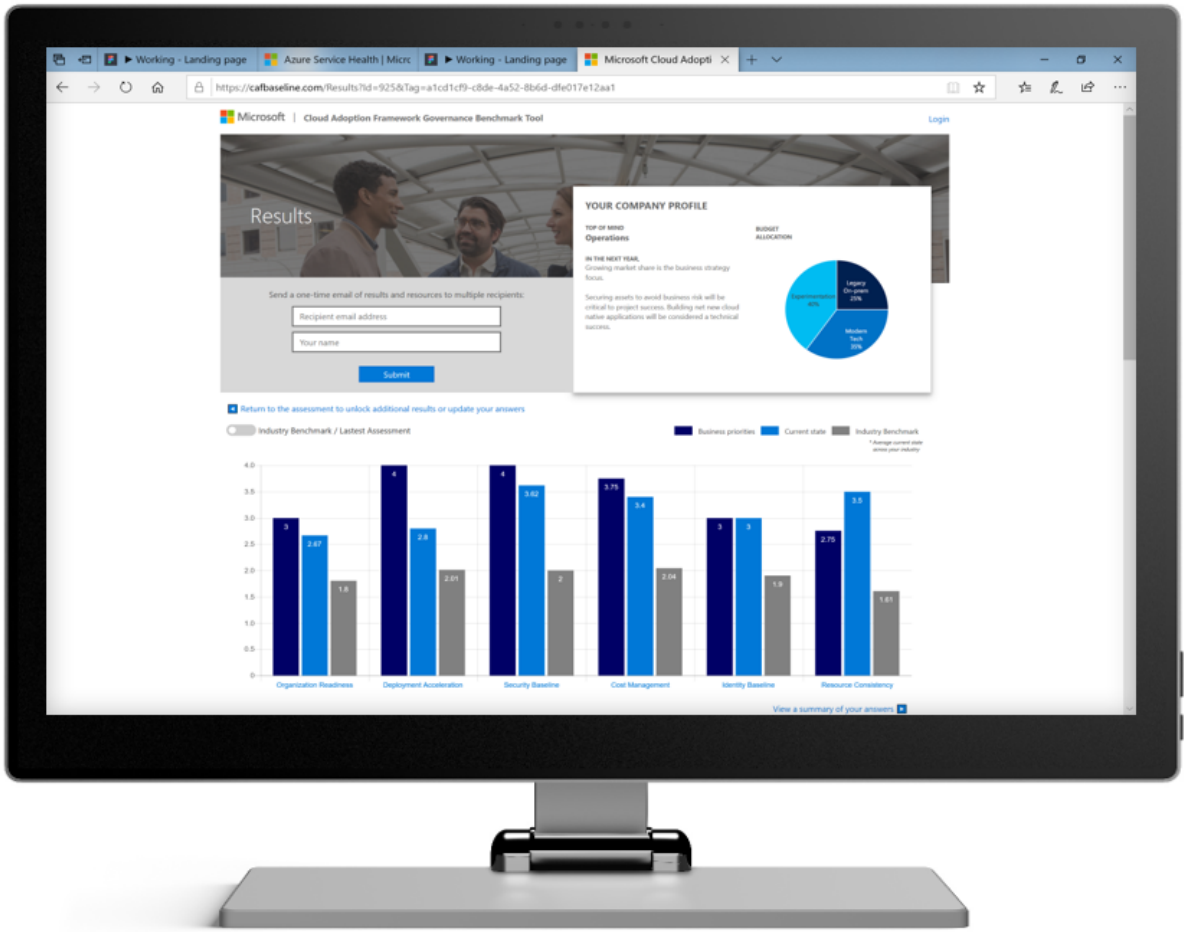


Figure 2: A governance benchmark output that shows areas for improvement and a comparison between current state and future state governance requirements.

Use the governance benchmark tool for a personalized report that outlines the difference between your current state and business priorities, along with tailored resources to help you start assessing your current state and future state and establish a vision for applying the framework.

Governance foundation

Azure includes a suite of governance tools that are built on top of the Azure Resource Manager platform. The initial governance foundation demonstrates how you can apply these tools to demonstrate cloud governance. As you progress through the units of this module, you'll learn how to apply these tools to solve governance challenges. First, start with a governance foundation to familiarize yourself with the tools.

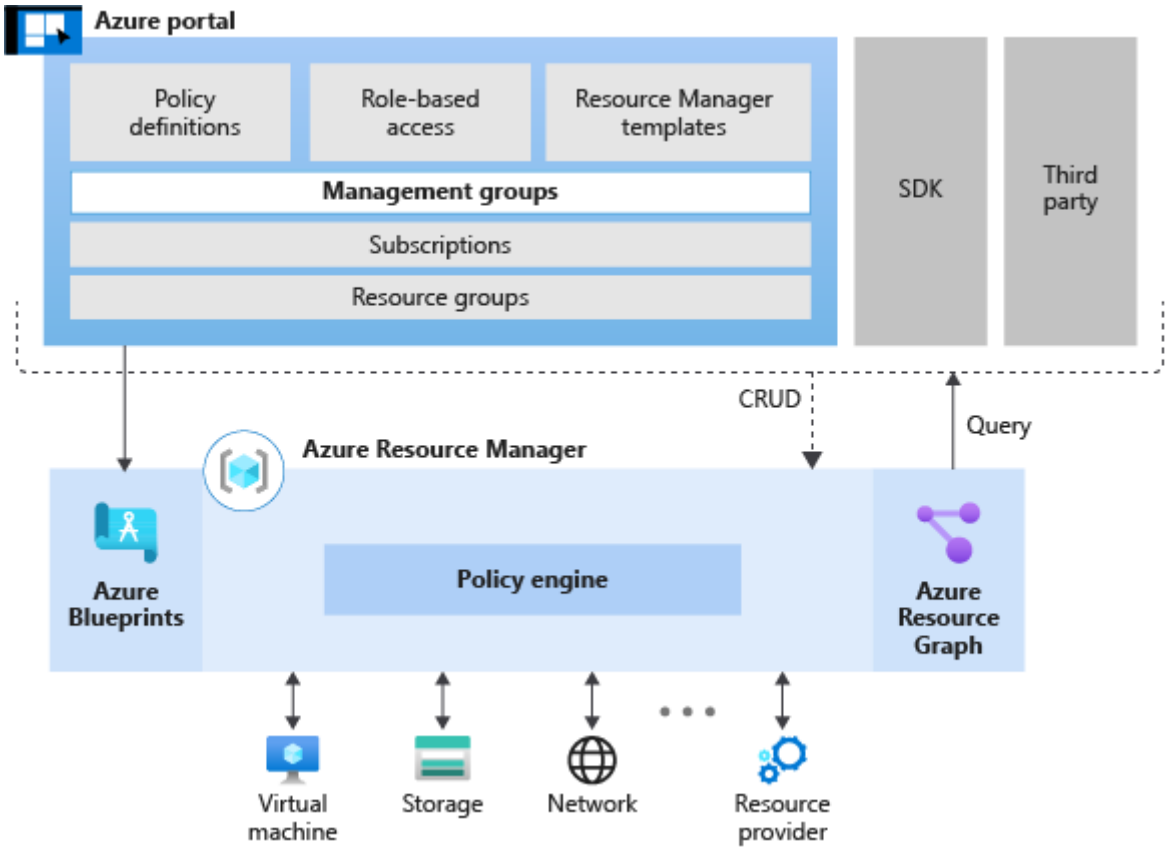


Figure 3: The Azure Resource Manager tools that support governance, with a focus on Azure Policy and Azure Blueprints.

In later units, you'll apply these tools to create a governance foundation for Tailwind Traders.

The Cloud Adoption Framework contains two ways to apply a sound foundation for governance to new or existing deployments. Each provides a different approach to support your business needs when you get started:

- Standard governance guide: A guide for most organizations that's based on the recommended initial two-subscription model, and designed for deployments in multiple regions while not spanning public and sovereign/government clouds
- Governance guide for complex enterprises: A guide for enterprises that are managed by multiple independent IT business units or span public and sovereign/government clouds

Mature governance disciplines

A governance foundation introduces you to tools that are needed to implement proper governance. To achieve sustainable governance, you'll need to apply guardrails for each governance discipline. To be more precise and more effective, teams should start with a single discipline and expand over time. The following table can help mature the disciplines that are needed to meet specific business objectives:

Risk/need	Standard enterprise	Complex enterprise
Sensitive data in the cloud	Discipline improvement	Discipline improvement
Mission-critical applications in the cloud	Discipline improvement	Discipline improvement
Cloud cost management	Discipline improvement	Discipline improvement
Multicloud	Discipline improvement	Discipline improvement
Complex/legacy identity management	N/A	Discipline improvement
Multiple layers of governance	N/A	Discipline improvement

Later in this module, we'll discuss each discipline from the Cloud Adoption Framework Govern methodology and relate them to Tailwind Traders' customer narrative.

Check your knowledge

1. Tailwind Traders currently has this policy in place: *Customer and financial data can only be hosted in a specific network segment of the existing datacenters, referred to as protected assets.* Is it a well-structured, scalable, and actionable policy?

○ Yes

- ◉ No

✔ **Correct! This policy is not well structured and would create a number of issues during cloud adoption.**

2. Which part of the Govern methodology in the Cloud Adoption Framework should be the first step in addressing the existing policy?

- ○ Deploy a governance foundation to set up governance tools in Azure.
- ◉ Advance the Security Baseline discipline to mimic the on-premises policy in Azure.

✘ **Incorrect. You might get close to meeting this policy requirement with a sound security baseline, but the team still would be bound to keep sensitive data and apps in the existing datacenter.**

- ○ Update the corporate policy to address the risks and concerns in non-technical terms.

✔ **Correct! Learning the tools and addressing security concerns are both important. But no amount of automated tooling can overcome poorly aligned corporate policies.**

Next unit: Corporate policies

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Corporate policies

20 minutes

Poor governance policies create unnecessary constraints, and they might not protect the company. This unit evaluates ways to create proper, actionable corporate policies.

Tailwind Traders' improper corporate policy

What's wrong with Tailwind Traders' existing policy, from the customer narrative?

Tailwind policy: *Customer and financial data can only be hosted in a specific network segment of the existing datacenters, referred to as protected assets.*

Corporate policies are designed to instruct teams on the best way to address tangible risks that the organization deems not tolerable. Corporate policies aren't designed to require a specific technical implementation.

Evaluate existing corporate policy

When you evaluate existing corporate policies to apply them to the cloud or to any other new technology, you should be able to answer the following questions:

- What risk does this policy attempt to mitigate?
- Why is that risk not within organizational risk tolerance?
- Who determined that the risk isn't tolerable?
- When should this policy be applied (workload classification, situational, and so on)? When should exceptions be reviewed?
- How is this process enforced? How often should the policy be reviewed for applicability?
- For technology-focused processes, does this policy add risk by creating a dependency on a specific technology solution or technology vendor?

As you'll see in the next unit, the Tailwind Traders policy on protected data fails to answer these questions. Some of them might be addressed elsewhere, like in policy handbooks, but the final technology-focused question is an undeniable miss. Instead of mitigating risk, it actually introduces long-term risks by locking in a single solution.

Define corporate policy

Defining corporate policy requires a focus on identifying and mitigating business risks, regardless of the cloud platform the organization uses. Healthy cloud-governance strategy begins with sound corporate policy. The following three-step process guides the iterative development of sound corporate policies:

Business risk: Investigate current cloud adoption plans and data classification to identify risks to the business. Work with the business to balance risk tolerance and mitigation costs.
Policy and compliance: Evaluate risk tolerance to inform minimally invasive policies that govern cloud adoption and manage risks. In some industries, third-party compliance affects initial policy creation.
Processes: The pace of adoption and innovation activities will naturally create policy violations. Executing relevant processes will help to monitor and enforce adherence to policies.

Business risk

During cloud adoption, you'll encounter various risks. Here are some examples of risks that might evolve at different points of your adoption effort:

- During early experimentation, a few assets with little to no relevant data are deployed. The risk is small.
- When the first workload is deployed, risk increases a little. This risk is easily remediated by choosing an inherently low-risk application that has a small user base.
- As more workloads come online, risks change at each release. New applications go live and risks change.
- When a company brings the first 10 or 20 applications online, the risk profile is much different than when the thousandth application goes into production in the cloud.

Risk is relative. A small company with a few IT assets in a building that's offline has little risk. Add users and an internet connection with access to those assets and the risk intensifies. When that small company grows to Fortune 500 status, the risks are exponentially greater. As revenue, business processes, employee counts, and IT assets accumulate, risks increase and

coalesce. IT assets that help generate revenue are at tangible risk of stopping that revenue stream if an outage occurs. Every moment of downtime equates to loss. Likewise, as data accumulates, the risk of harm to customers grows.

According to the outline from the Tailwind Traders customer narrative unit, here are the risks the Tailwind CIO is most concerned about:

- Overspending in the cloud
- The organization not meeting security or compliance requirements
- Asset configuration creating operations-management issues or oversights
- Unauthorized access compromising systems or data
- Inconsistent governance due to immature processes and lack of skills on the team

It's important to note that none of the concerns are related to "a specific network segment of the existing datacenters," as cited in Tailwind's current policy. To create sound governance policies that scale to the cloud, we need to dig a bit deeper and look at the tangible risks that are captured in the current policy versus the current-state solution.

Deeper investigation of stakeholder concerns and the cloud-adoption plan likely will show more risks that the organization can't tolerate. But for now, we have enough to start shaping governance policies that address these tangible risks.

Policy and compliance

Corporate policies establish the requirements, standards, and goals that your IT staff and automated systems need to support. Individual policy statements are guidelines for addressing specific risks that are identified during your risk assessment process. Here are a few examples of proper corporate policies that guide adoption in public and private cloud deployments, and which avoid locking in a specific vendor:

- **Avoid overspending**: Cloud deployments involve a risk for overspending, especially for self-service deployments. Any deployment must be allocated to a billing unit, with an approved budget and with a mechanism for applying budgetary limits.

  Design consideration: In Azure, budget can be controlled with Microsoft. Azure Advisor can provide optimization recommendations to reduce spending per asset.

- **Secure sensitive data**: Assets that interact with sensitive data might not receive sufficient protections, leading to potential data leaks or business disruptions. All assets that interact with sensitive data must be identified and reviewed by the security team to ensure that proper levels of protection are in place.

Design consideration: In Azure, all deployed assets must be tagged with proper data classification levels. Classifications must be reviewed by the cloud governance team and the application owner before deployment to the cloud.

Process

The cloud provides guardrails to help reduce the human overhead of recurring processes by providing validation triggers based on implementation configuration. The following table outlines a few triggers and actions that can address the risks that concern the Tailwind Traders CIO:

Risk	Sample trigger	Sample action
Overspending in the cloud	Monthly cloud spending is 20 percent higher than expected	Notify the billing unit leader, who will start reviewing resource usage
Overspending in the cloud	Deployed assets aren't using the allocated CPU or memory	Notify the billing unit leader and automatically resize to fit actual usage, when possible
The organization not meeting security or compliance requirements	Detect any deviation from defined security or compliance	Notify the IT security team and automate remediation, when possible
Asset configurations creating operations management issues or oversights	CPU utilization for a workload is greater than 90 percent	Notify the IT operations team and scale out additional resources to handle the load
Asset configurations creating operations management issues or oversights	Assets that fail to meet patching or business continuity and disaster requirements trigger operational compliance warning	Notify the IT security team and automatically resolve the deviation, when possible
Unauthorized access compromising systems or data	Traffic patterns deviate from approved network topologies	Notify the IT security team and automatically close attack vectors, when possible

Risk	Sample trigger	Sample action
Unauthorized access compromising systems or data	Assets are configured without proper role assignments or elevated privileges	Notify the IT security team and automatically resolve the deviation, when possible
Inconsistent governance due to immature processes and lack of skills on the team	Assets identified that aren't included in required governance processes	Notify the IT governance team and automatically resolve the deviation, when possible

You can automate each of these triggers and actions by using Azure governance tools. Other cloud providers might require a more manual approach, but the defined policies would still be applicable. Take care to avoid defining policies that would lock you into using a specific vendor to avoid having to repeat this process again in the future.

After establishing your cloud policy statements and drafting a design guide, you'll need to create a strategy to ensure that your cloud deployment stays in compliance with your policy requirements. This strategy must encompass your cloud-governance team's ongoing review and communication processes, establish criteria for when policy violations require action, and define the requirements for automated monitoring and compliance systems that will detect violations and trigger remediation actions.

In the next unit, we'll group these types of risks into actionable cloud disciplines.

Next unit: Governance disciplines

Continue >

100 XP

Governance disciplines

3 minutes

Common governance disciplines within cloud platforms inform policies, align toolchains, and help organizations determine how best to automate and enforce corporate policies across their unique cloud platforms.

The following table summarizes each discipline from the Govern methodology in the Cloud Adoption Framework:

Cost Management discipline: Cost is a primary concern for cloud users. Develop policies for cost control for all cloud platforms.
Security Baseline discipline: Security is a complex subject that's unique to each company. Once security requirements are established, cloud-governance policies and enforcement apply those requirements across network, data, and asset configurations.
Identity Baseline discipline: Inconsistencies in the application of identity requirements can increase the risk of breach. The Identity Baseline discipline focuses ensuring that identity is consistently applied across cloud-adoption efforts.
Resource Consistency discipline: Cloud operations depend on consistent resource configuration. Through governance tooling, resources can be configured consistently to manage risks related to onboarding, drift, discoverability, and recovery.
Deployment Acceleration discipline: Centralization, standardization, and consistency in approaches to deployment and configuration improve governance practices. When provided through cloud-based governance tooling, they create a cloud factor that can accelerate deployment activities.

Resource Consistency discipline

Cost Management discipline

This discipline focuses on scaling the operational best practices for cost management across all workloads and assets in your portfolio.

This discipline would help Tailwind Traders address the following risk:

- Overspending in the cloud

Later, we'll demonstrate how Tailwind Traders can add cost controls to its governance foundation.

Security Baseline discipline

This discipline focuses on automating the application of security principles to ensure consistency across your environment.

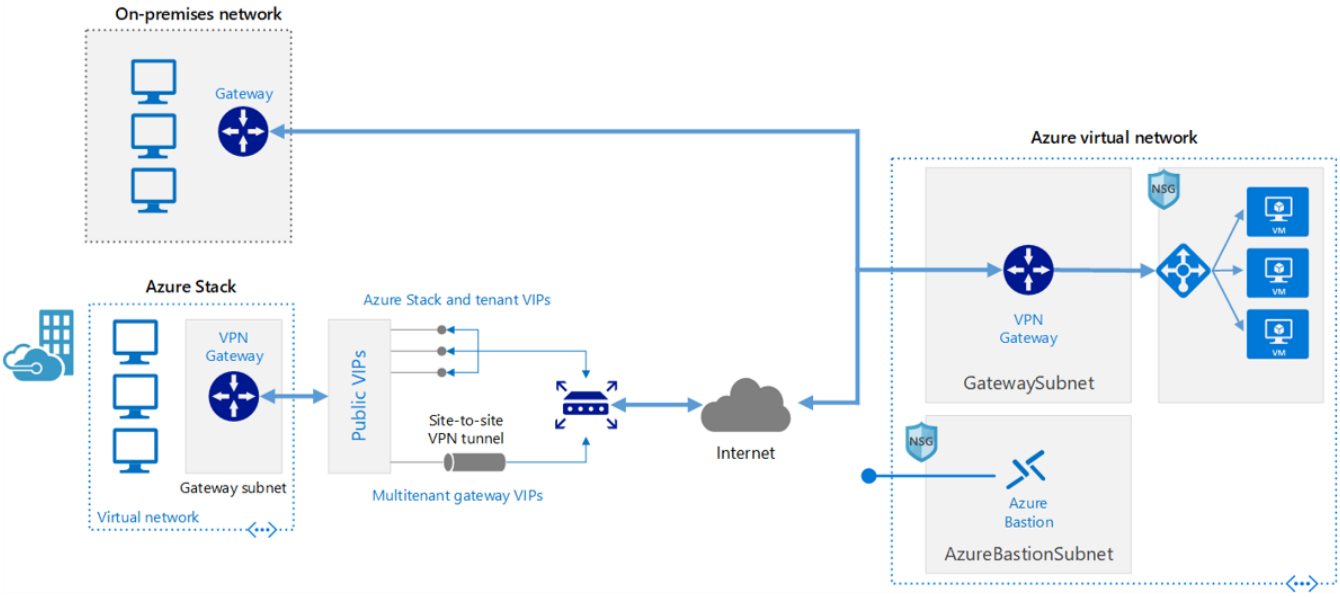


Figure 2: The Security Baseline discipline.

This discipline would help Tailwind Traders address the following risks:

- The organization not meeting security or compliance requirements
- Unauthorized access compromising systems or data

Identity Baseline discipline

After you've established identity and access requirements for your cloud environment, this discipline ensures that those requirements are consistently applied to all workloads and assets.

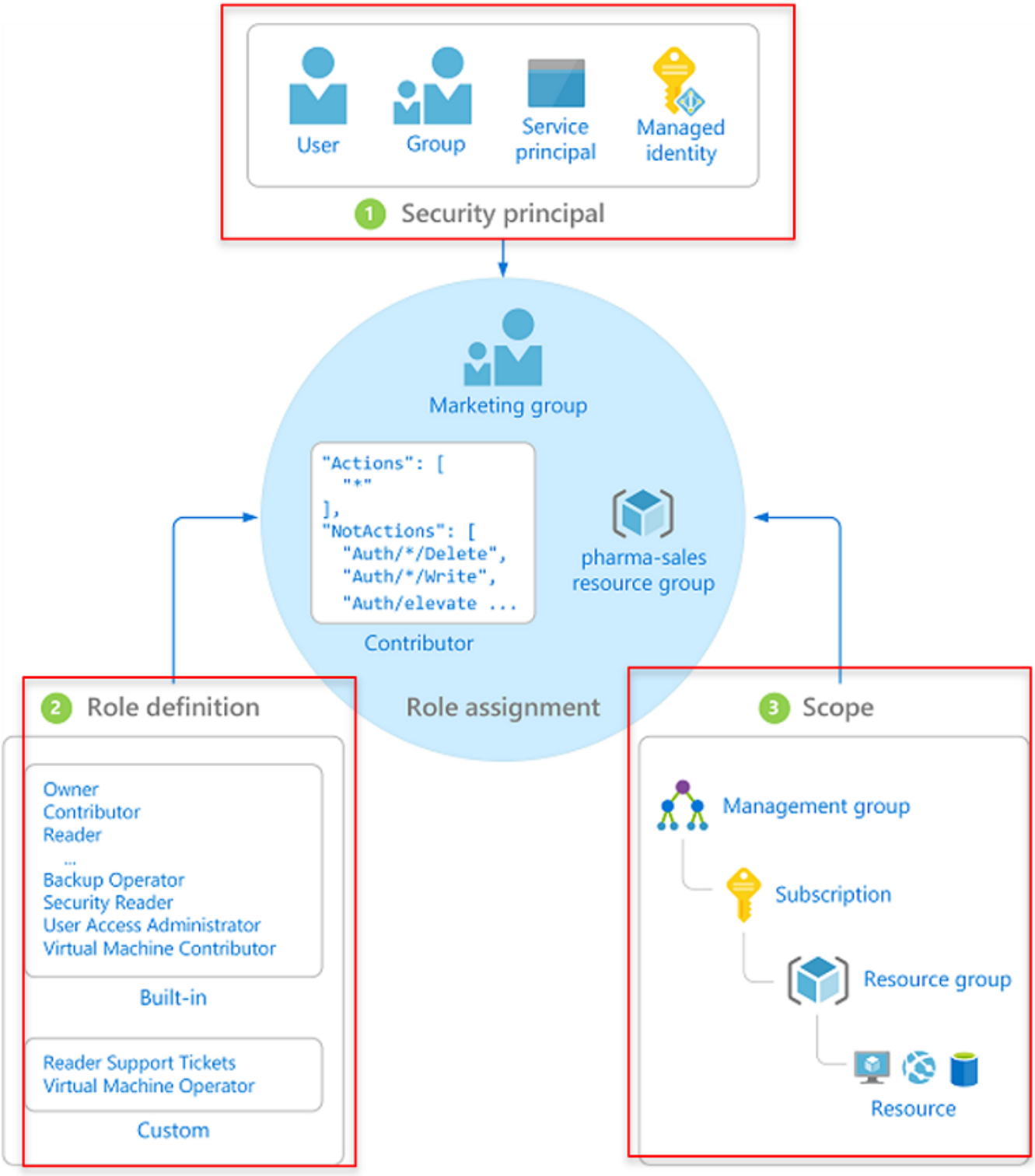


Figure 3: The Identity Baseline discipline.

This discipline would help Tailwind Traders to address the following risk:

- Unauthorized access compromising systems or data

Resource Consistency discipline

Resource consistency focuses on the initial organization of the resources that are required to establish a foundation for governance. In the long term, this discipline focuses on proper onboarding processes to ensure that all assets meet any operational support requirements.

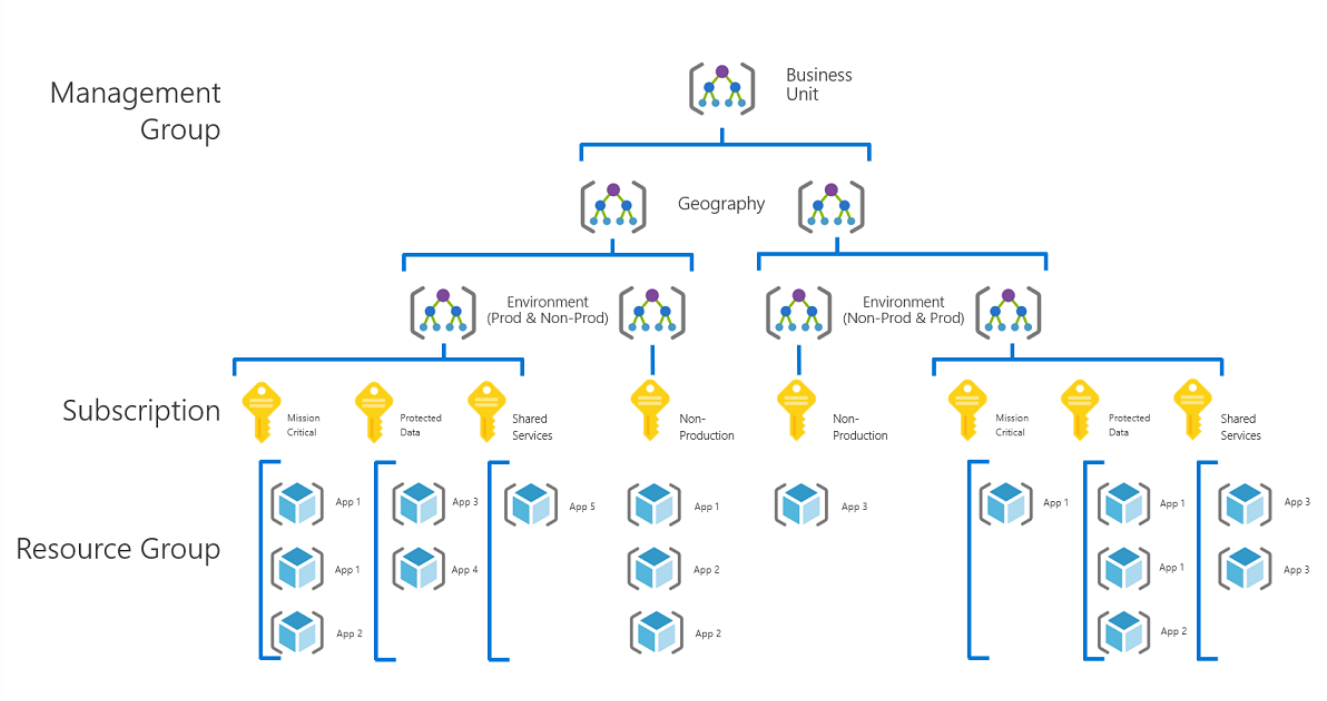


Figure 1: The Resource Consistency discipline.

This discipline would help Tailwind Traders address the following risks:

- Operations management issues or oversights

Later, we'll apply this discipline to the early needs of our customer narrative for Tailwind Traders.

Deployment Acceleration discipline

Automating governance leads to automation in adoption. Providing infrastructure as code (IaC) templates to the various adoption teams helps them quickly deploy workloads into compliant, well-managed environments.

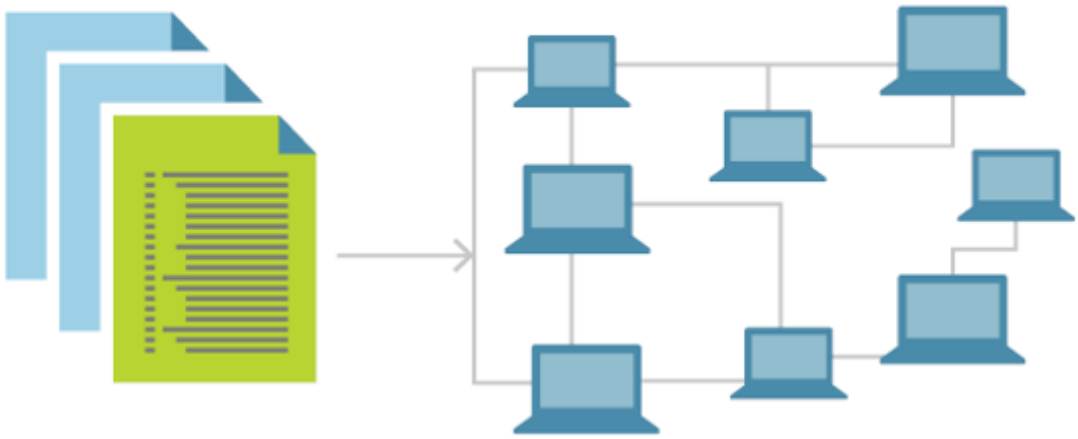


Figure 4: The Deployment Acceleration discipline.

This discipline would help Tailwind Traders to address the following risk:

- Inconsistent governance due to immature processes and lack of skills on the team

The five disciplines of the Govern methodology in the Cloud Adoption Framework help establish the right collection of processes, tools, and automation to address common risks and concerns. Understanding these disciplines can help Tailwind Traders discover and address tangible risks and concerns, and then address them against a prioritized backlog.

In the next units, we'll explore technical solutions to help you get started with a cloud-governance foundation to support each discipline. We'll also look at some technical solutions that address risks related to managing costs.

Next unit: Knowledge check

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

Knowledge check

10 minutes

Test your knowledge about the first few steps toward sound Azure governance.

The following questions help you think through which actions Tailwind Traders can or should take. The questions also help you reflect on what various stakeholders think overall about cloud governance.

Which comes first? What matters most?

1. To address the risks and concerns the Tailwind Traders CIO raises in the customer narrative, which of the following steps would you start with?

- ○ Implement a governance foundation in Azure.
- ◉ Update the existing corporate policy to outline concerns, risks, triggers, and actions.

  ✔ **Correct! Starting with sound corporate policy will make all downstream implementations smoother.**
- ○ Deploy cost management controls and processes.
- ○ Deploy security baseline controls and processes.

2. Which would you address second?

- ○ Implement a governance foundation in Azure.

  ✔ **Correct! A governance foundation will implement tools and references to begin building cloud governance solutions.**
- ◉ Update the existing corporate policy to outline concerns, risks, triggers, and actions.

  ✘ **Incorrect. Corporate policy should be at the top of a list of things to address.**
- ○ Deploy cost management controls and processes.
- ○ Deploy security baseline controls and processes.

3. Which will deliver the most visible improvement based on existing corporate policy?

- ○ Implement a governance foundation in Azure.
- ○ Update the existing corporate policy to outline concerns, risks, triggers, and actions.
- ○ Deploy cost management controls and processes.
- ◉ Deploy security baseline controls and processes.

✔ **Correct! In the customer narrative, the visible pain points can be addressed through an automated security baseline to reduce security risks.**

4. Which will increase confidence for the CIO?

- ○ Implement a governance foundation in Azure.
- ○ Update the existing corporate policy to outline concerns, risks, triggers, and actions.
- ◉ Deploy cost management controls and processes.

✔ **Correct! In this narrative, the CIO expresses concerns with cost. Addressing those concerns by adding cost management controls will build confidence.**

- ○ Deploy security baseline controls and processes.

Next unit: Deploy a cloud governance foundation

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Deploy a cloud governance foundation

10 minutes

Deploying a cloud-governance foundation accelerates your ability to govern your entire Azure environment. This unit outlines the considerations and implementations that are required to deploy a foundation that can achieve resource consistency and prepare you for other governance disciplines.

What will you configure?

This unit assumes that you've already deployed assets to Azure. Now, you want to configure the environment to better organize, track, and govern those assets. When you finish this unit, you'll understand *why* and *how* to configure management groups, subscription design, resource groups, and tagging.

Strategic considerations

Resource organization is based on what's important to your organization. Before you define a management group or subscription design, it's important to understand the priority of these competing priorities:

- **Cost transparency**: Every cloud adoption should be aligned to departments, business units, projects, or other cost allocation mechanisms for chargeback and showback accounting requirements
- **Compliance and security**: Every cloud adoption should map to specific compliance requirements that map cloud adoption to specific risk, security, and compliance organization structures
- **Democratization (delegated responsibility)**: Every cloud adoption should map to teams, product groups, or projects for easier segmentation of responsibility by teams

Understanding these strategic priorities can help you identify the best starting point for your management and subscription design.

Resource organization in Azure

The basic foundation of all governance is consistent resource organization.

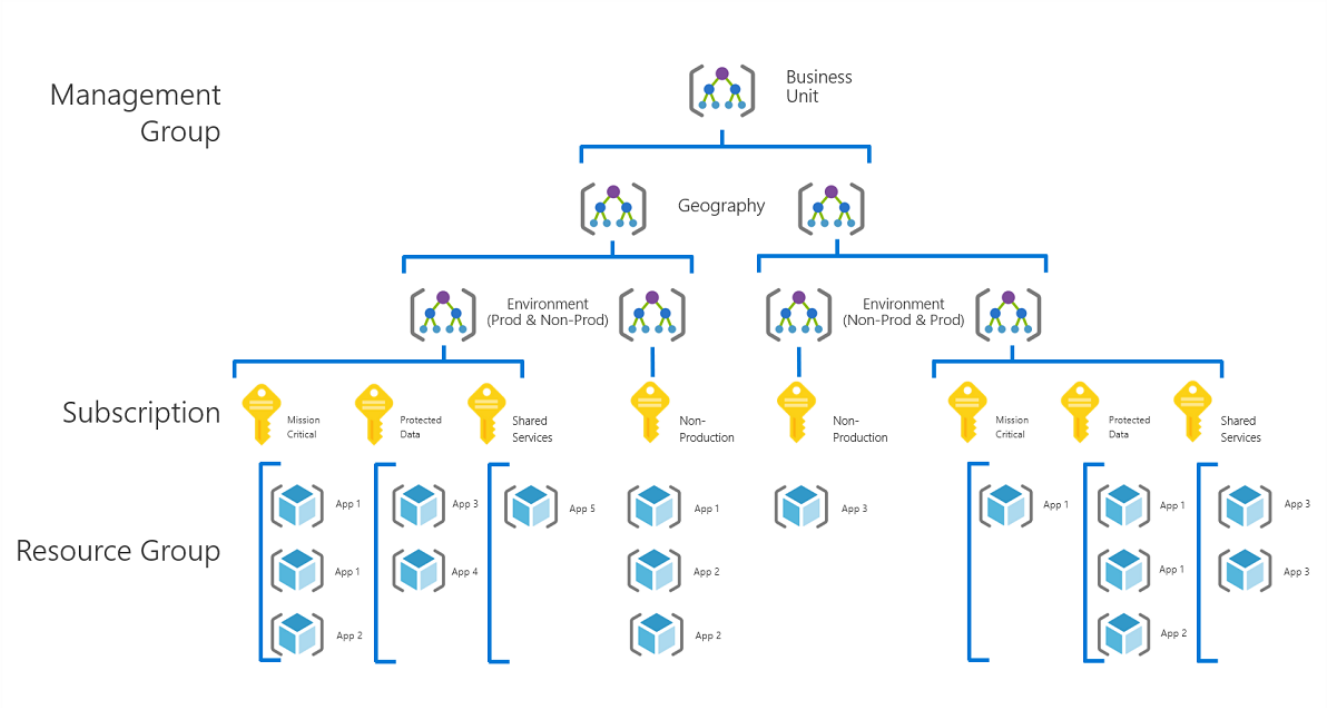


Figure 1: Resource consistency.

The three main components of resource organization are:

- *Management groups*, which reflect security, operations, and business or accounting hierarchies
- *Subscriptions*, which group similar resources into logical boundaries
- *Resource groups*, which further group applications or workloads into deployment and operations units

Governance design consideration

To accommodate long-term governance needs, design a high-level hierarchy, but implement only what you need. Add new nodes to the hierarchy as requirements dictate.

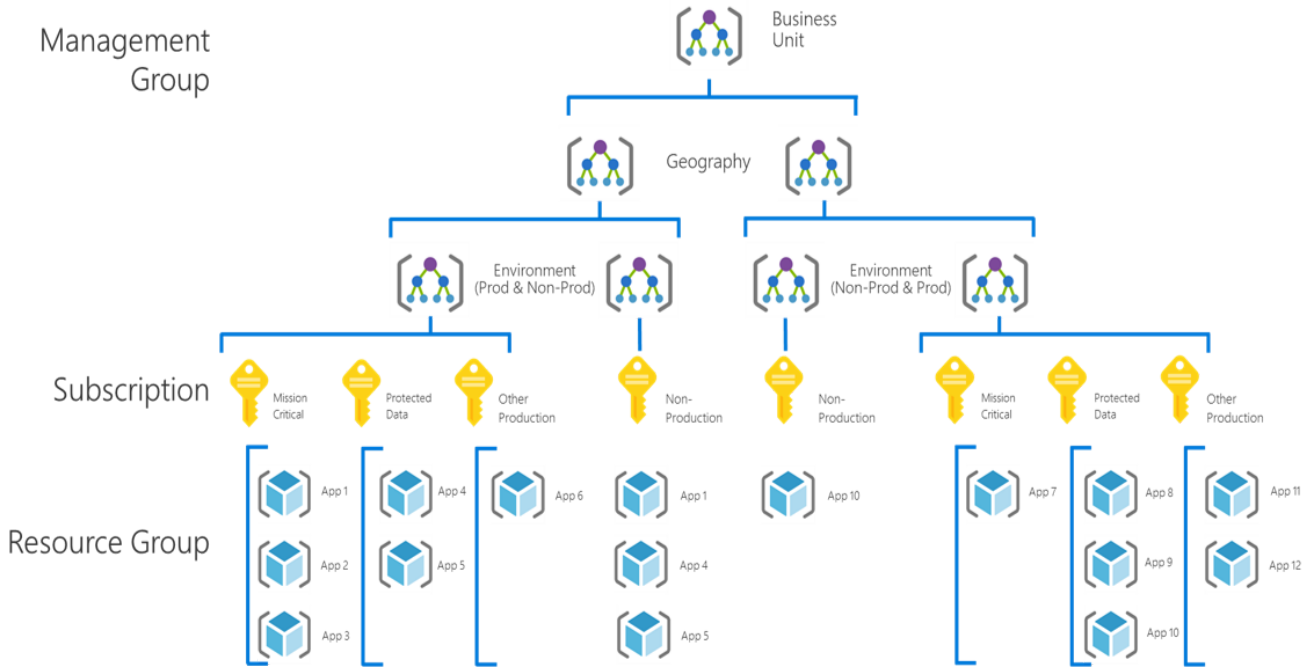


Figure 2: Management group hierarchy.

The following components are in descending levels in the management group hierarchy shown in Figure 2:

- **Management group**: Business unit, geography, and environment
- **Subscription**: Per application category, pre-production, development environments, and production
- **Resource groups**: Per application

Exercise: Configure your first management group hierarchy

Start with a smaller hierarchy so you can experiment and quickly overcome initial learning curves.

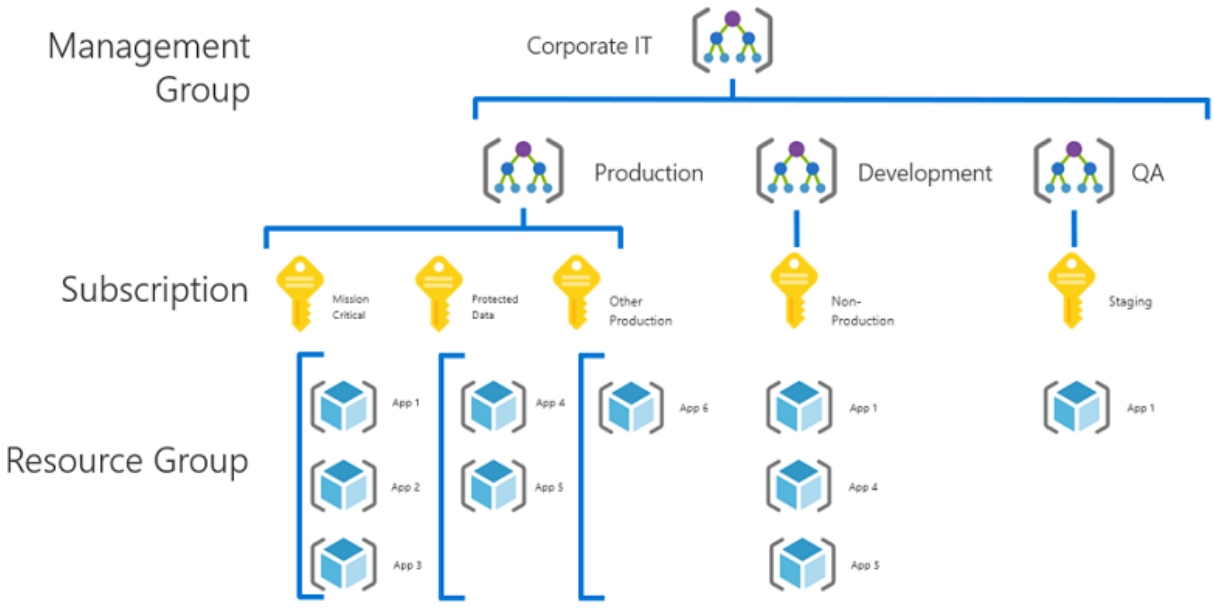


Figure 3: Initial, smaller management group hierarchy.

In this smaller version, attempt the following configuration steps:

- **Parent node**: Define a management group for corporate IT
- **Child nodes**: Define child nodes for each production and nonproduction environment

For guidance on creating these management groups, see the quickstart guide for creating a management group in the Azure portal.

Subscription design

A subscription is a logical container for all deployed assets. Subscriptions are used to group together common workloads based on billing, compliance, security, or access requirements. To maximize the effectiveness of governance, you should use as few subscriptions as possible.

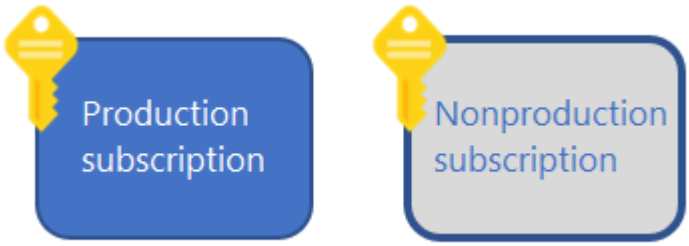


Figure 4: Production and nonproduction subscriptions.

Scaling with subscriptions

There are several technical and non-technical reasons to scale with multiple subscriptions. See the fundamental concepts article for an overview of common reasons to scale.

The following questions might help illustrate reasons for you to scale your subscriptions:

- Are there capacity or technical limitations?
- Do you need to clearly separate concerns? For example:
  - Separation of duties
  - Dev/test versus generic nonproduction
  - Different customers
  - Different departments or business units
  - Different projects
- Will you be able to spread the cost of a shared infrastructure across application owners? (Often, a dedicated subscription is used for shared infrastructure, like Azure Active Directory, monitoring, or patching tools.)

- Do you need to create clearer separation of duties through shared service subscriptions for operations management, security, identity sync, connectivity, or DevOps teams?

Exercise: Add subscriptions to your management groups

Add existing subscriptions in each of the environment nodes to create clarity between production, development, and QA resources.

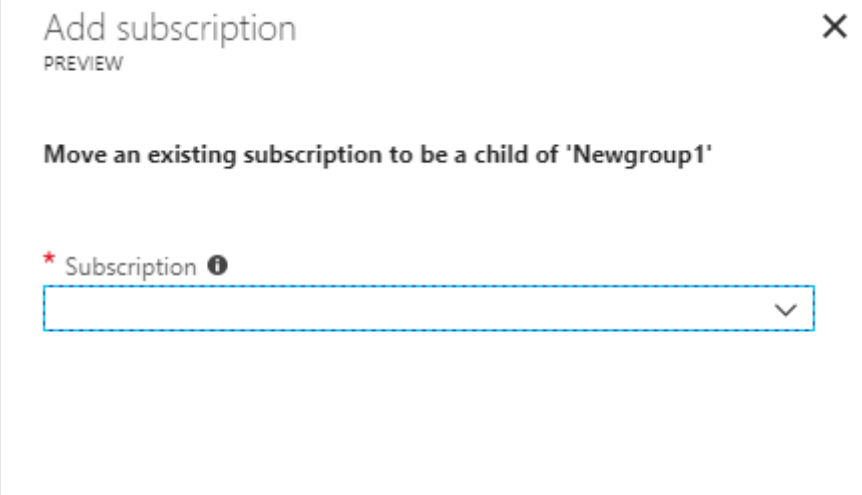


Figure 5: Add a subscription to a management group.

For guidance on adding subscriptions to a management group, see the how-to guide.

Tagging

Management groups reflect your highest-priority organization structure. Tagging reflects various organizing principles that also are reflected in metadata. Here are suggested tags for all workloads:

- Workload (and/or application)
- Data sensitivity; see Data classification for examples
- Mission criticality; see Workload criticalityfor examples
- Owner
- Department (cost center)
- Environment

Exercise: Assign a tagging policy

You can apply Azure policies to all subscriptions in a management group. To understand the role of policy in your governance foundation, apply a policy to one of your management groups in the hierarchy.

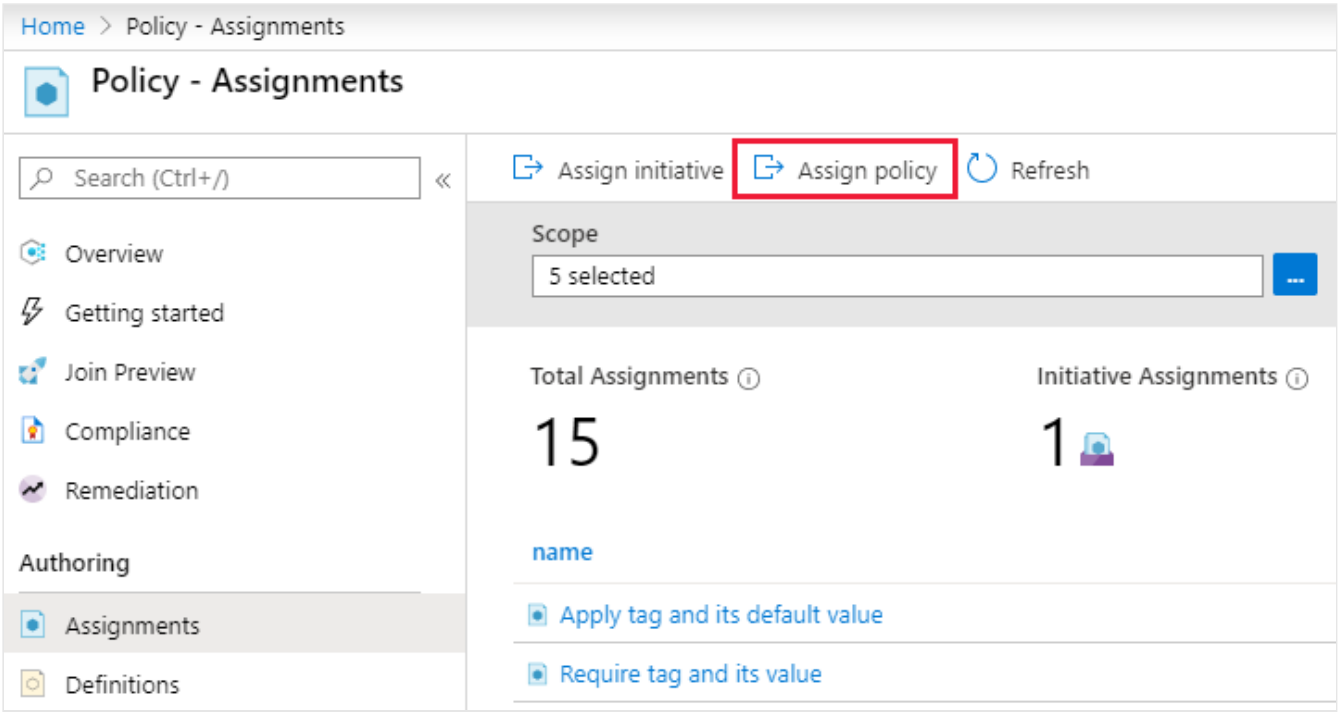


Figure 6: Assign a policy in the Azure portal.

For guidance on applying a policy, see the tutorial on creating and managing policies

- Step 4 of the instructions for assigning a policy discusses scope. This is where you will select the management group to ensure that the policies are applied to all subscriptions in the management group.
- Steps 6 and 7 discuss policy definition. From the list of **Built-in** policies, we suggest selecting one of the policies related to tagging. Specifically, the policy that requires a tag on all resources will help establish a governance foundation.

> **Important**
>
> Step 9 in the **tutorial** illustrates **Policy enforcement**. As you learn about governance, be sure to set **Policy enforcement** to **Disabled**. When this setting is disabled, you can audit your environment without making any changes, and it won't prevent future deployments.

Deployment acceleration

Packaging all the governance change in a blueprint accelerates deployments and creates consistent governance application. When we assign a blueprint in the next exercise, governance is consistently applied to all subscriptions in the assigned management group and to all resource groups and assets in those subscriptions.

Exercise: Assign the CAF Foundation blueprint

Use Azure Blueprints to package Azure Resource Manager templates, Azure policies, and role-based access control settings into a single package. The Cloud Adoption Framework for Azure (CAF) Foundation blueprint provides an example and a starting point for using blueprints in cloud governance to:

- Deploy Azure Key Vault
- Deploy Log Analytics in Azure Monitor Logs
- Deploy Microsoft Defender for Cloud (standard version)

The CAF Foundation blueprint also defines and deploys policies to:

- Apply `cost center` tags to resource groups
- Append resources in resource group with the `cost center` tag
- Permit an Azure region for resources and resource groups
- Permit storage account SKUs (choose when deploying)
- Permit Azure Virtual Machines SKUs (choose when deploying)
- Require Azure Network Watcher to be deployed
- Require secure transfer encryption for Azure Storage accounts
- Deny resource types (choose when deploying)
- Create an initiative to enable monitoring in Microsoft Defender for Cloud (89 policies)

Follow the prescribed steps to publish and assign this sample blueprint to your management group.

Exercise: Evaluate a current environment

Customers commonly attempt to add governance to existing, mature adoption efforts across multiple subscriptions. As you mature your governance practices across a portfolio, the Azure governance visualizer can provide insights about your current governance configuration.

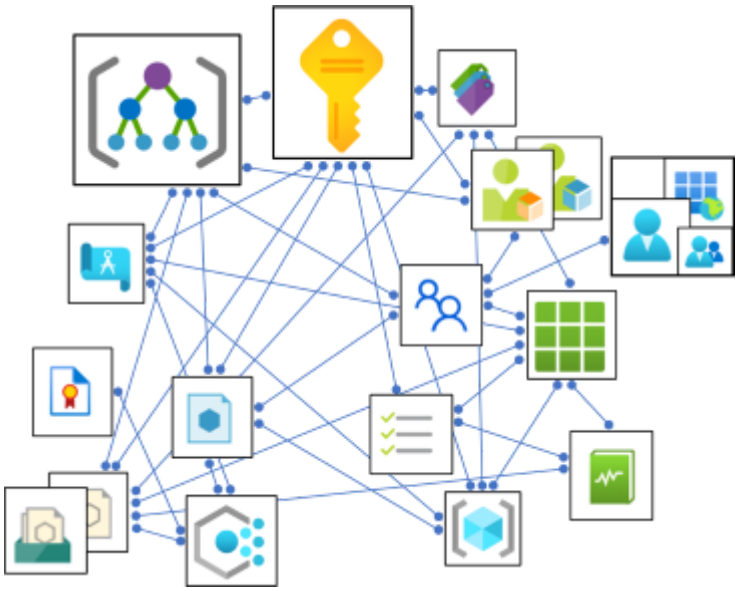


Figure 7: The Azure governance visualizer.

Deploy the Azure governance visualizer to see how management groups, blueprints, policies, and other governance configurations have been applied across your environment.

These exercises help demonstrate a starting point or foundation for governance. In the next unit, you'll build on this foundation to establish a mature Cost Management discipline.

Next unit: The Cost Management discipline

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

The Cost Management discipline

10 minutes

Cost management often is the first discipline that customers choose to mature in any governance engagement. This unit outlines the outcomes, tools, processes, and a reference implementation to mature your cost discipline.

Objective

The Cost Management discipline builds confidence in your ability to control costs and respond to the following triggers:

- Address concerns about budgets
- Define cost allocation across business units
- Implement cost guardrails
- Analyze workload costs
- Apply operational best practices across your portfolio
- Create accountability for cost best practices with each workload team

Cost management best practices

The objective of this discipline is to apply these cost management best practices:

- Align teams and accountability
- Manage best practices centrally
- Establish best practices for workload levels

Best practices by team and accountability

Cost management across the enterprise is a function of cloud governance and cloud operations. All cost-management decisions change the assets that support a workload. When those changes affect a workload's architecture, additional considerations are required to minimize the impact on users and business functions. It's likely that the cloud-adoption team that configured or developed that workload will be accountable for following through with those changes.

- **Tagging is critical to all governance**: Make sure that all workloads and resources follow proper naming and tagging conventions and that you enforce tagging conventions by using Azure Policy.
- **Identify right-size opportunities**: Review your current resource utilization and performance requirements across the environment.
- **Resize**. Modify each resource to use the smallest instance or SKU that can support the performance requirements of each resource.
- **Horizontal versus vertical scale**: Using multiple small instances can give you an easier scaling path than a single larger instance. Using multiple smaller instances supports scale automation, which creates cost optimization.

Operational cost management best practices

The following best practices typically are achieved by a member of the cloud-governance or cloud-operations team in accordance with patching and other scheduled maintenance processes. These best practices map to actionable guidance we describe later in this unit.

- **Tagging is critical to all governance**: Ensure that all workloads and resources follow proper naming and tagging conventions and that you enforce tagging conventions by using Azure Policy.
- **Identify right-size opportunities**: Review your current resource utilization and performance requirements across the environment to identify resources that have remained underutilized for more than 90 days.
- **Right-size provisioned SKUs**: Modify underutilized resources to use the smallest instance or SKU that can support the performance requirements of each resource.
- **Autoshutdown for virtual machines (VMs)**: When a VM isn't used constantly, consider automated shutdown. The VM won't be deleted or decommissioned, but it will stop consuming compute and memory costs until it's turned back on.
- **Autoshutdown for all nonproduction assets**: If a VM is part of a nonproduction environment, specifically in a development environment, establish an auto-shutdown policy to reduce the cost of non-use. Whenever possible, use Azure DevTest Labs as a self-service option to help developers hold themselves accountable for cost.
- **Shut down and decommission unused resources**: Yes, we said it twice. If a resource hasn't been used in more than 90 days and doesn't have a clear uptime requirement, turn it off. More importantly, if a machine has been stopped or shut down for more than 90 days, deprovision and delete that resource. Validate that any data-retention policies are met through backup or other mechanisms.
- **Clean up orphaned disks**: Delete unused storage, especially VM storage that's no longer attached to a VM.
- **Right-size redundancy**: If the resource doesn't require a high degree of redundancy, remove geo-redundant storage.

- **Adjust autoscale parameters**: Operational monitoring likely will uncover usage patterns for various assets. When those usage patterns map to the parameters that are used to drive autoscale behaviors, it's common for the operations team to adjust autoscale parameters to meet seasonal demand or changes to budget allocations. Review workload cost management best practices for important precautions.

Workload cost management best practices

Before making architectural changes, consult the technical lead for the workload. Facilitate a review of the workload by using the Azure Well-Architected Framework overview and introduction to guide decisions about the following architectural changes:

- **Azure App Service**: Verify production requirements for any Premium tier App Service plan. Without an understanding of the business requirements for a workload and the underlying assets configuration, it's difficult to determine whether a Premium tier plan is required.
- **Horizontal versus vertical scale**: Using multiple small instances can give you an easier scaling path than a single larger instance. Using small instances supports scale automation, which creates cost optimization. Before a workload can scale horizontally, the technical team must verify that the application is idempotent. Achieving horizontal scale might first require changes to the code and configuring various layers of the application.
- **Autoscale**: Enable autoscale on all app services for a burstable number of smaller VMs. Enabling autoscale has the same idempotent requirement, which requires an understanding of the workload architecture. The workload and supporting assets must be approved for horizontal scaling and autoscaling by the cloud-adoption team before any operational changes are made.
- **Implement serverless technologies**: VM workloads often are migrated as-is to avoid downtime. Often, VMs host tasks that are intermittent, tasks that take a short period to run, or tasks that run for many hours. Examples are VMs that run scheduled tasks like Windows task scheduler or PowerShell scripts. When these tasks aren't running, you're still paying for the VMs and disk storage. After migration, consider rearchitecting layers of the workload as serverless technologies, like by using Azure Functions or Azure Batch jobs.

Cost management process

The best practices described here are actionable, but how and when do you apply them? The Cost Management discipline is a continuous effort that involves multiple processes and roles.

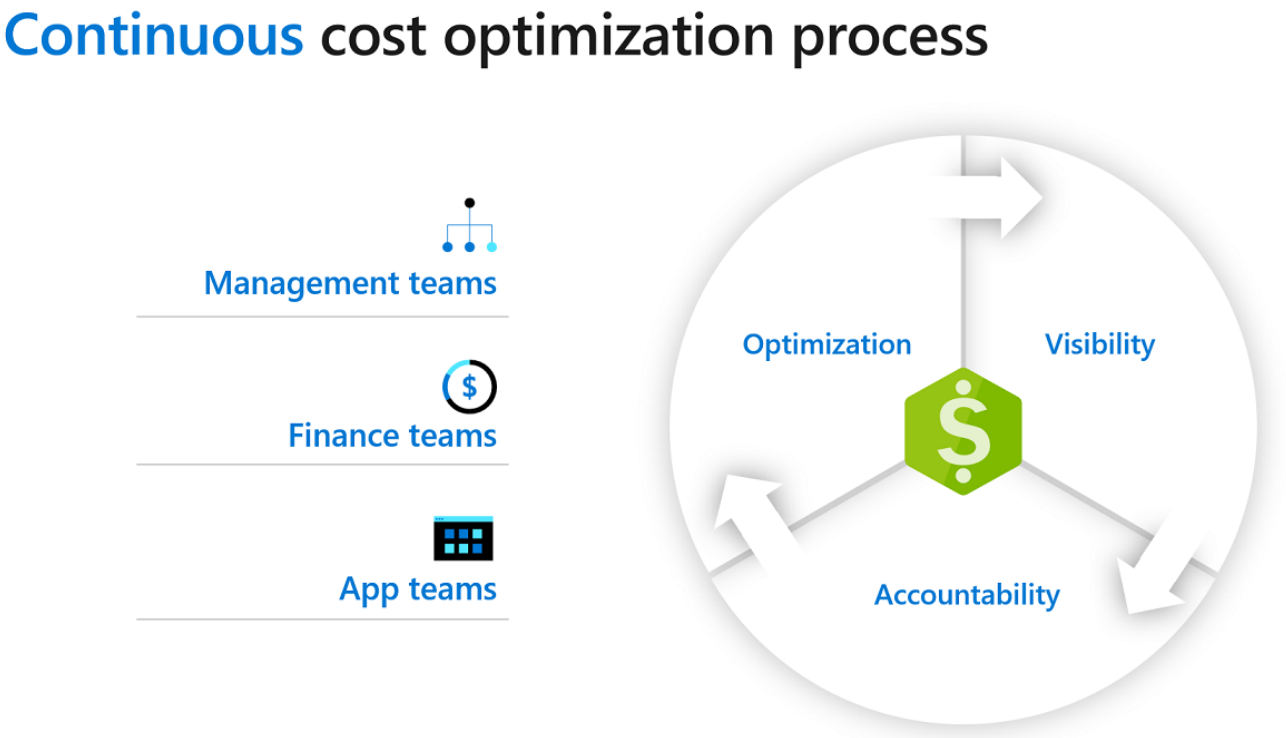


Figure 1: The Cost Management discipline as a continuous process.

Work with the central operations and workload teams to ensure proper ownership of each Cost Management discipline best practice that's shown in Figure 1 (optimization, visibility, accountability). Depending on how you manage workloads in your environment, some best practices might move between teams. Although some organizations place all the cost management burden on central IT and neglect accountability for the workload team, other organizations place all the cost management burden on the workload team. Most organizations fall somewhere between these two extremes. At Tailwind Traders, central IT serves only a reporting and budget-management function.

After you align roles, establish recurring processes to meet and hold each other accountable for this important recurring task.

Microsoft Cost Management

Microsoft Cost Management is your default tool in Azure to bring together all the data for managing your cost strategy.

Microsoft Cost Management brings together resource organization, Azure Advisor alerts, and your governance foundation to meet your cost management needs.

Exercise: Create a budget

To get started with Microsoft Cost Management, create your first budget with the Create and manage Azure budgets tutorial.

Exercise: Find opportunities to optimize

If you have existing deployments in your Azure environment, you likely have recommendations in the Azure portal that might affect your overall spending. Complete the Optimize costs from recommendations tutorial to view recommendations from Azure Advisor and other recommendations that might reduce your costs. The recommendations identify opportunities to apply the operational best practices described in this unit.

Exercise: Limit cost risks by using Azure Policy

To proactively limit unexpected costs, you can use Azure Policy to create guardrails that affect the ability of any role to overspend. The two most common cost risks come from misunderstood decisions:

- **Azure regions**: Asset costs vary between Azure regions. When possible, you can use Azure Policy to limit deploying resources across regions.
- **Azure SKUs**: The SKU that's selected during deployment directly affects costs. Minimizing the use of expensive resources in self-service or workload-owned subscriptions can limit surprise budget overrun.

Add a policy to deny VM SKUs in your nonproduction environments to see this type of cost control policy in action.

Add a policy to specify allowed locations for specific subscriptions to avoid cost drift related to regional pricing.

Next unit: Summary

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Introduction

5 minutes

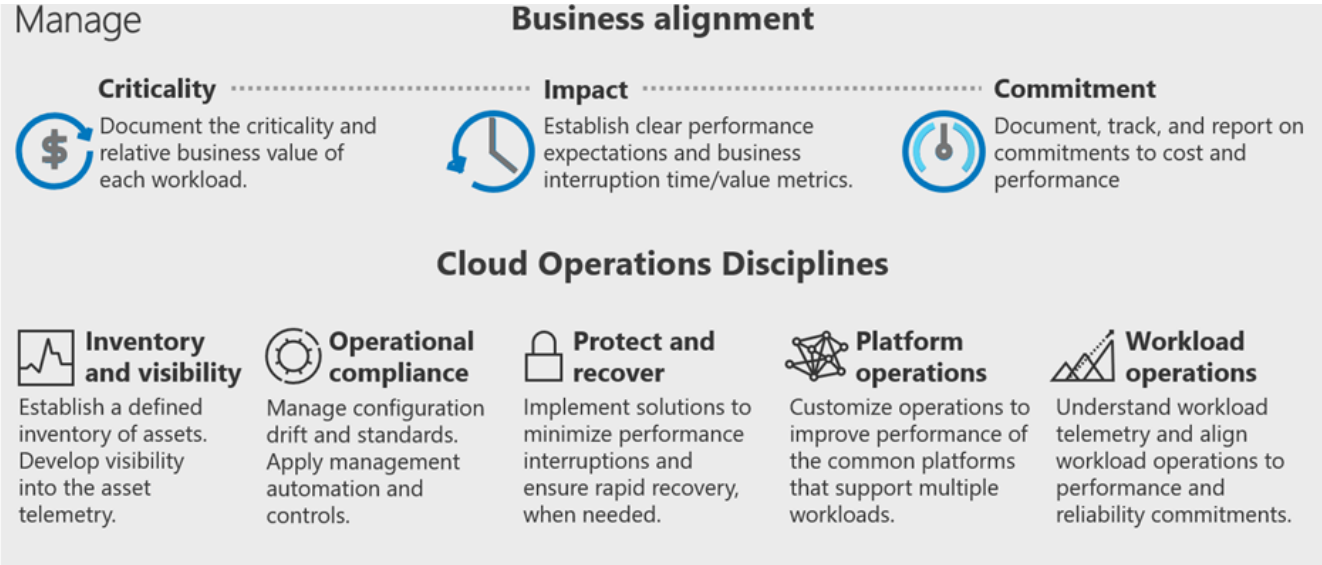
As a business moves to a cloud-based model, the importance of proper management and operations can't be overstated. In Azure, it's possible to visualize what management solutions cost per workload. In other words, the business can balance management cost against how critical the workload is to the business.

A management baseline is the minimum set of tools applied to all resources in the environment. This module walks through the three disciplines in a cloud-management baseline:

- **Inventory and visibility:** Inventorying assets and creating visibility into the run state of each resource of a workload
- **Operational compliance:** Management of configuration, sizing, cost, and performance of assets
- **Protection and recovery:** Data protection and quick recovery to minimize operational interruptions

The start of this module looks into business alignment to make sure everyone uses the same terms. The module then covers how to enhance the management baseline. The end of the module reviews the specialization principles. Workload specialization and platform specialization can support the most critical workloads and platforms.

The following image shows the components of a management baseline that this module covers.



Module scenario

Suppose you work as an IT operations architect at a company that has been migrating two datacenters to Azure. In this process, the company wants to modernize IT operations and its IT management solution. You use the guidance in this Learn module to evaluate how a cloud-native solution will support the company's cloud journey.

The new cloud-native solution will include a management baseline for the cloud environment. The fundamental management baseline will be for all workloads, and will have extra features for specific platforms and workloads. The solution should also enable reporting on management costs for the business stakeholders.

Learning objectives

In this module, you'll:

- Set a baseline for criticality, impact, and commitment for your business
- Understand which Azure management tools to include in a management baseline
- Learn how to partner with workload and platform teams for more prosperous decentralized operations

Prerequisites

- Foundational understanding of cloud adoption
- Understanding of your organization's requirements for operations management

---

Next unit: Establish business commitments

100 XP

Establish business commitments

10 minutes

The first step in creating business alignment is ensuring that everyone uses the same terms. Most likely, the engineers in the IT department don't use the same words as business stakeholders.

Developing a cloud strategy is a perfect opportunity to align these terms and look into commitments between IT and the business. The following three words will help improve the conversation with business stakeholders: *criticality*, *impact*, and *commitment*.

After all teams are aligned on terms, you should document and store that information for easy access.

Criticality

How critical is the workload for the business? If you ask users, most will say that their daily workload is the most critical one. But this conversation needs to be held from a business overview perspective.

A company-wide scale for criticality makes sure everyone involved in the conversation means the same thing. The following list is an example of a criticality scale:

- **Mission-critical:** The workload affects the company's mission and might noticeably affect corporate profit-and-loss statements.
- **Unit-critical:** The workload affects the mission of a specific business unit and its profit-and-loss statements.
- **High:** The workload might not affect the company's mission, but affects high-importance processes.
- **Medium:** Impact on processes is likely. Losses are low or immeasurable, but brand damage or upstream losses are possible.
- **Low:** Impact on business processes isn't measurable. No brand damage or upstream losses are likely. Localized impact on a single team is expected.
- **Unsupported:** No business owner, team, or process associated with this workload can justify any investment in the workload's ongoing management.

Some workloads might not be classified as critical, but can be vital indirectly. For example, if a non-critical compliance-management tool goes offline, maintaining business-critical compliance requirements is challenging. It can affect the company's mission in the long run.

A workload can also be critical because customers who bring the most income use it. Another soft-cost factor can be that the board or CEO is using the workload daily.

Instead of walking through every workload, you can decide one default criticality (for example, medium) for all workloads. A default criticality makes it easier to identify workloads that need higher or lower criticality classification.

Impact

The business needs to understand what an outage will cost. The output of the impact conversation is used to balance investments for cloud management.

The most common metric for impact is *impact per hour*, meaning operating revenue losses per hour of outage. To estimate impact per hour, you can look into historical data if an outage happened earlier. Also work with the finance department to determine the best approach to estimate loss per hour. If you can't find any financial data, you can use the percentage of affected customers to measure impact.

Commitment

Documented commitments between the business and IT create a true partnership. All businesses have workloads that are key to the company. If any of these key workloads fail, the entire company will be affected. On the other side of the scale, some workloads can be offline for months without any notice. These workloads should be managed in different ways.

Business commitments are about finding the balance between the level of operational management and operating cost. For most workloads, a baseline level is enough. Critical workloads make it easier to justify double management costs because of any business interruption's potential impact.

Management baseline

The first business commitment comes in the form of a promise to deliver a set level of services for operations management. Those services are called a *management baseline*. Based on the services included in the baseline, central IT can easily calculate a minimum service-level agreement (SLA) that will apply to everything deployed to a controlled cloud platform.

Management of higher-impact areas

The second business commitment focuses on what else is needed from operations for various platforms and workloads. Any platform or workload with higher levels of criticality or impact will likely need more than the minimum SLA.

To complete the business commitment, it's important to document who will be responsible for managing higher levels of day-to-day operations for those workloads. It can be a centralized responsibility with a central IT team or a mixed model between different groups.

Next unit: Deploy an operations baseline

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Deploy an operations baseline

10 minutes

The discipline of operational compliance is the cornerstone for maintaining the balance between security, governance, performance, and cost. Effective operational compliance requires consistency in a few critical processes:

- **Resource consistency:** If all resources are organized the same way and tagged the same way, other management tasks become more manageable.
- **Environment consistency:** If all landing zones are organized the same way, both management and troubleshooting become much more manageable.
- **Resource configuration consistency:** As with resources and landing zones, it's crucial to monitor resource configuration. If a configuration setting is changed, it can trigger an automation job to restore the environment.
- **Resource optimization:** Regular monitoring of resource performance will reveal trends in resource utilization and opportunities to optimize the cost and performance of each resource.
- **Update consistency:** All updates to the environment should be done in a scheduled, controlled, and possibly automated way. Controlled change management will reduce unnecessary outages and troubleshooting.
- **Remediation automation:** Automation for quick remediation of common incidents is a great way to increase customer satisfaction and minimize outages. Known issues should be fixed by their root cause. Fixing a root cause is often a long process, and automation is a quick fix.

Operational compliance can be fulfilled per workload: for example, in one of your landing zones.

The following table lists some of the Azure tools for operational compliance. Remember that not all of these tools need to be part of the default management baseline.

Tool	Description	Link to more information

Tool	Description	Link to more information
Azure Automation Update Management	Management and scheduling of updates	Update Management overview
Azure Policy	Policy enforcement to ensure environmental and guest compliance	Azure Policy overview
Azure Blueprints	Automated compliance for core services	Azure Blueprints overview
Azure Automation State Configuration	Automated configuration on the guest OS and some aspects of the environment	State Configuration overview

Next unit: Protect and recover

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Protect and recover

10 minutes

Protection and recovery are the third and final discipline in a cloud-management baseline. For an enterprise environment, this table outlines the suggested minimum for any management baseline:

Tool	Description	Link to more information
Azure Backup	Backup of data and virtual machines in Azure	Azure Backup overview
Microsoft Defender for Cloud	Strengthened security and advanced threat protection	Microsoft Defender for Cloud product page

Another essential tool is Azure Site Recovery. Azure Site Recovery replicates virtual machines and workloads between clouds, Azure regions, or local datacenters. When an outage occurs in your primary Azure region, your workload (for example, virtual machines) fails over to the copy running in the secondary Azure region. The workload will then be online in the secondary site or region.

This approach to recovery can significantly reduce recovery times. Most likely, the default management baseline includes Azure Site Recovery. For your most critical workloads, it can be suitable protection.

An older IT environment often has one backup solution with one configuration. Azure makes it easy to deploy a backup vault for each workload if needed. With separate backup vaults, you can handle both permissions to backup data and showback for the backup cost.

Next unit: Enhance an operations baseline

Continue

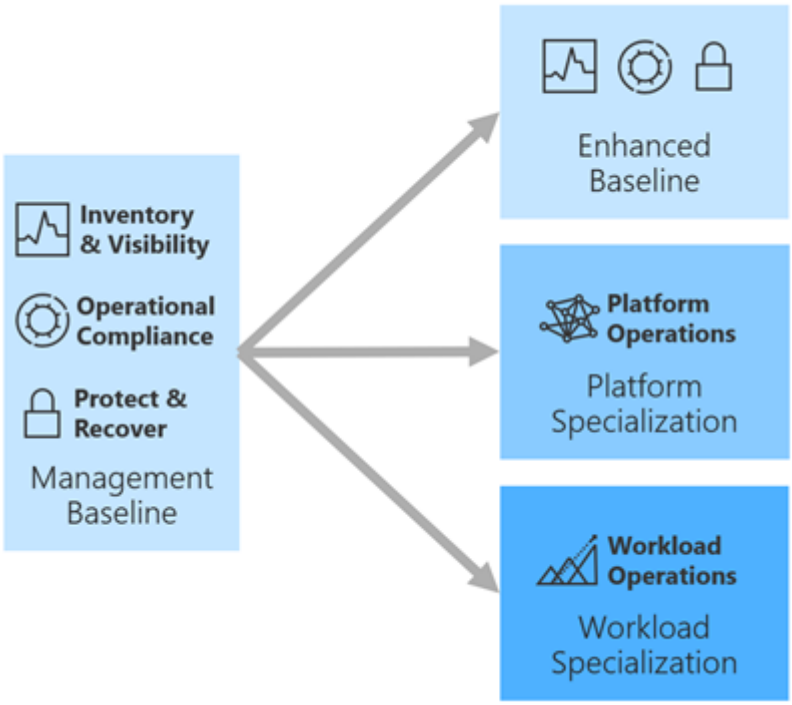
100 XP

Enhance an operations baseline

10 minutes

So far in this module, we've talked about the three cloud-management disciplines, which we call a management baseline. This unit will look beyond the default management baseline.

There are most likely workloads in your environment that require more management services than what's described in the management baseline. An *enhanced* management baseline is often a low operations investment, compared to workload or platform specialization.



If most of your workloads require more than your default management baseline, reviewing the management baseline is a good idea. A management baseline review is also a good idea when new services are implemented or new features of Azure are released. For example, if your company implements an IT service management (ITSM) solution, a connection to automate incident creation adds to the enhanced operations baseline.

Workload specialization is for the most mission-critical workloads. This is about 20 percent of the workloads.

Platform specialization is for the platform or platforms that run the most high-criticality workloads. The specialized platform investment is often divided over many workloads.

The following table shows some of the most common enhancements to a management baseline:

Tool	Description	Link to more information
Azure Resource Graph	Visibility into changes to Azure resources that might help detect negative effects sooner or remediate faster	Azure Resource Graph product page
IT Service Management Connector	Automated ITSM connection to create awareness sooner and enrich work items	IT Service Management Connector overview
Azure Automation	Automation of: • Responses to changes • Resource-specific scaling or sizing issues • Operations across multiple clouds	Azure Automation product page
Azure Automation State Configuration	Code-based configuration of guest operating systems to reduce configuration drifting and quickly find errors	State Configuration overview
Microsoft Defender for Cloud	Extended protection to include recovery triggers for security breaches	Microsoft Defender for Cloud product page

Next unit: Manage platform and workload specialization

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Manage platform and workload specialization

10 minutes

Workload specialization

Workload-specific management usually requires in-depth knowledge about the specific workload. That's why it's often done by the workload team or development team. A workload-specific solution does not scale quickly to other workloads. Centralized IT can still guide and share knowledge with the workload-specialized team on operations.

Platform specialization

Decentralized, workload-specific operations aren't scalable across an enterprise. But a study of the portfolio will often identify common platforms on which those workloads run. Those technology platforms (also known as technology stacks) are often at the heart of workload-specific incidents. When priority workloads share a common technology platform, it might be more valuable for central IT to focus on improving the operations of those platforms, and thereby reduce or avoid workload-specific operations.

Examples of technology platforms might include data platforms, analytics platforms, container platforms, Azure Virtual Desktop platforms, enterprise resource planning (ERP) platforms, or even mainframes.

Advanced operations

Platform and workload specialization consists of disciplined execution of the following four processes in an iterative approach:

- **Improve system design:** Technical debt and architectural flaws are the root cause of most business workload outages. By reviewing the platform or workload design, you can improve stability. The Azure Well-Architected Framework includes recommendations for improving the quality of the platform or a specific workload.

- **Automate remediation:** Some design improvements aren't cost-effective, because the technical debt can be too costly or complex to improve. In such cases, it might make more sense to automate remediation and reduce the effect of interruptions.
- **Scale the solution:** As system design and automated remediation are improved, those changes can be scaled across the environment through the service catalog. Publish optimized platforms and solutions in Azure Managed Applications Center to easily reuse them for other workloads or external customers.
- **Continuously improve:** Collecting feedback from users, administrators, and customers will give you valuable information for the next system review. Collecting and visualizing critical system logs and performance data are also important. Both the feedback and the data collected will be used as a foundation for making new decisions about future system improvements.

The following table shows tools used for workload-specific management:

Tool	Description	Link to more information
Application Insights	Advanced application monitoring with dependency mapping, application dashboard, application map, usage, and deep tracking	Application Insights overview

Next unit: Knowledge check

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

Knowledge check

10 minutes

Check your knowledge

1. Which are the three keywords in working with business alignment?

- ○ Criticality, impact, and commitment

  ✔ **Criticality, impact, and commitment are the three keywords to align with the business.**

- ◉ Criticality, responsibility, and response

  ✘ **The three keywords in a management baseline don't include responsibility or response.**

- ○ Criticality, impact, and owners

2. What is a management baseline?

- ○ A policy to control a management tool for a specific Azure resource
- ◉ A free version of the Azure management suite

  ✘ **A management baseline is often one or more tools applied to all resources in the environment.**

- ○ The minimum set of tools applied to all resources in the environment

  ✔ **The first step in creating business alignment is to ensure term alignment.**

3. What is impact often measured in?

- ○ The most common time/value metric is impact per hour.

  ✔ **A time/value metric measures operating revenue losses per hour of outage.**

- ◉ The most common time/value metric is impact per workload.

✗ **In this scenario, impact measurement is for the business, not for a workload or platform.**

○ The most common time/value metric is impact per platform.

4. How would you describe commitment as part of a management baseline?

○ Business commitments are about finding the balance between the level of operational management and operating cost.

✓ **Commitments, criticality, and impact are the keywords in business alignment.**

◉ Commitments are the SLA for each management baseline.

✗ **The three keywords in a management baseline don't include SLA.**

○ Commitments are the SLA for each management tool in a management baseline.

5. When is Application Insights a recommended tool?

○ When working with data protection

◉ When working with workload-specific management

✓ **Application Insights can give deep insight into applications.**

○ When working with an essential management baseline

Next unit: Summary

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Introduction

3 minutes

Tailwind Traders is now facing competitive pressure for its products from startups that have entered the online retail market. Early customer feedback indicates that these new entities offer a better online experience than Tailwind Traders.

Industry trends show that the growth of the online market is higher than the growth of brick-and-mortar businesses. So, Tailwind Traders has reprioritized innovation efforts to reshape its digital presence and e-commerce platforms.

One obstacle is the large effort that the existing applications require to introduce modifications. Besides, Tailwind Traders' experience shows that application changes often result in application downtime and a reduced customer experience.

The change rate has traditionally been slow for Tailwind Traders' applications. The new competitive threats in the e-commerce sector demand a higher innovation speed and as much uptime as possible.

Tailwind Traders wants to rearchitect the on-premises applications after migrating them to Azure with a lift-and-shift process. The goal is to reach the required innovation rate that will allow for the company to survive in the new competitive ecosystem.

Next unit: Follow the innovation lifecycle

Continue

100 XP

Follow the innovation lifecycle

5 minutes

Tailwind Traders has questions about innovation that affect many other organizations too:

- How do we increase the rate of change without affecting the running business?
- How do we decide where to innovate and what changes to implement, to maximize the business return of those innovations?

The answer to both questions is that Tailwind Traders needs to embrace change as part of its organizational culture. One reason why change-averse organizations often have change-related outages is that those changes are too large and impactful. The changes are hard to test in controlled and realistic environments.

If processes are established to introduce changes frequently, those changes will be smaller in size and risk. However, this process does not just involve adopting certain tools or technologies. It requires a culture that fosters change and accepts failures.

The concept of accepting failures might seem counterintuitive, but it's vital to the innovation cycle. If people are afraid to fail because errors will put them at the center of blame games, new approaches to problem solving will likely not be pursued in the fear of failure. The whole organization will then be a prisoner of its established practices.

It's possible to establish a "fail fast" culture where people are encouraged to try out new methods, and they're empowered to quickly change direction if they don't get the expected outcome. That will help create a richer innovation culture.

Hypothesis-based innovation

Innovation can be described as a hypothesis-based, iterative cycle. Upon identifying the existence of a problem, one or more hypotheses can be formulated that can potentially explain the root cause and lead to the solution. The definition of the problem itself can be challenging, because it needs to be measurable.

For example, the problem definition "Customers are not happy with our payment platform choices" isn't measurable, so it will be difficult to solve. If the problem can be defined as "23

percent of customers leave their shopping session at the step of choosing the payment platform," you're in a better position to measure the success of any possible solution.

After you define a problem in a measurable way, you can formulate hypotheses that are candidates for explaining and solving the problem. For example, a hypothesis for Tailwind Traders might be described as: "Adding ContosoPay to our supported payment platforms would decrease customer churn at the payment page from 23 percent to 10 percent." Now an idea is on the table, and acting on it is a matter of verifying its validity.

Hypotheses should focus on adding value to customers and improving their experience in their interactions with your organization. That's often known as "customer empathy": placing your customer at the center of your innovation, and focusing on increasing value for them and for you.

There are many ways to validate a hypothesis without touching application code. Customer surveys and market research are two examples of valuable information sources that can help to decide the validity of a hypothesis. Checking these sources will allow you to qualify your hypothesis, and to build hypotheses with highest likelihood of accuracy and added business value.

Build

After a hypothesis has enough value potential to be built into your application, the build process starts. Here again, speed is crucial.

Your development sprints should be as short as possible. Keeping sprints short allows quick verification or rejection of the hypothesis. It also potentially allows you to fine-tune the way in which the required functionality will be integrated in the application. The result is quicker innovation cycles.

Measure

You want to verify the accuracy of your hypothesis as soon as possible. A minimum viable product (MVP) is a preliminary version of the new functionality that gathers feedback and helps confirm whether you're moving in the right direction.

The goal of the MVP is verifying not only your hypothesis, but any assumptions you might have made, too. For example, if 23 percent of Tailwind Traders' customers leave the purchasing process at the payment page, the hypothesis holds that the reason is that the company isn't offering enough payment platforms. However, the reason might be different. The MVP should be designed to confirm or reject these assumptions and the hypothesis.

Learn

The learn phase is similar to the start of the process. After you learn more about your assumptions and hypothesis, you might find out that they were right, partially right, or wrong. Having a growth mindset and enough humility to admit failures will allow you to either:

- Quickly pivot if you need to continue working on your MVP
- Refocus your efforts in other areas and formulate an alternative hypothesis

It's important to realize that even if your assumptions and hypothesis were wrong, the process has allowed you to learn something new about your customers and your business. Don't think of it as wasted time. The key is gaining that knowledge as soon as possible and applying it to a future hypothesis. That's the core of the fail-fast culture.

Where to look next

The Innovation overview of the Cloud Adoption Framework is the best place to begin your exploration of how to innovate.

Next unit: Azure technologies for the build process

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Azure technologies for the build process

10 minutes

In this unit, you'll learn the relationship between the innovation process and some of the technologies in the industry that can help you to build new functionality into applications.

DevOps

After you've started the build phase to validate your innovation hypothesis, the required development, integration, and deployment cycles should be as streamlined as possible. This is where DevOps comes in. You can define DevOps as "processes and tools to deliver software features quickly and reliably." Here are details about this definition:

- **Processes and tools**: DevOps, and the innovation process as a whole, is based on culture patterns that encourage change. Azure and GitHub offer great tooling around DevOps, but purchasing a license isn't enough. Your processes and organizational culture need to evolve to embrace change and innovation.
- **Quick delivery of software features**: DevOps processes and tools embrace the concept of failing fast. Building MVPs or prototypes to quickly validate whether the feature on which you're working goes in the right direction is core to the concept of DevOps.
- **Reliable delivery of software features**: Change-averse organizations often associate quick changes with downtime. However, DevOps promises exactly the opposite: a quick change rate and a high level of reliability. This is possible by integrating testing in early stages of the development cycle, in a process called "shift to the left."

  If the development of a feature across time is seen as a line from left to right, a legacy development process would perform user validation and quality control at the end of the development cycle, or at the "right" end of that line. DevOps advises you to test and validate as early as possible, at the "left" of that time line.

DevOps embodies the same core concepts of a healthy innovation culture. Adopting its methodology is key to get to an agile innovation cycle.

Microservices architectures

Modularity is a well-known technique to reduce complexity in architecting complex systems. If a system is a complex interaction of many pieces that can't be taken apart (often called a "monolith"), tight component interdependencies will make system improvements difficult. Every change needs to be validated with the rest of the system, so the test process is complex.

If the system is modular, it can be separated into smaller subsystems that interact with each other via well-defined interfaces. Introducing changes in one of these subsystems is easier, because as long as its interface with the other modules stays constant, the overall system will continue working.

Microservices architectures are application patterns that exploit modularity. Applications are subdivided into separate, small components that can be developed independently from each other, potentially even using different programming languages. Each component, or microservice, can operate on its own. You can scale it as required, you can troubleshoot it as a single unit, you can modify it independently from the other microservices.

A question that organizations often ask is what to do if an application is monolithic. Should the organization redesign the application into a microservices architecture before introducing innovation, or can the innovation and redesign processes run in parallel? There is no single answer to this question. It depends on the complexity and business relevance of the application under consideration.

Tailwind Traders confronted this question when looking at introducing innovation in its e-commerce platform. The company decided to start a project to redesign the e-commerce application into a microservices architecture, because the application's business criticality justified this effort. Not having a modular application would severely impair Tailwind Traders' ability to react to changing trends in the online market.

However, Tailwind Traders has decided to tackle some of the major gaps in its platform at the same time. Waiting for the application redesign project to finish would mean losing significant market share to the new startups that are disrupting the ecommerce market right now.

The projects will interact with each other, guided by the business value of innovations. The redesign efforts will focus on the most critical application areas, where the need for modification to improve customer experience is highest.

Containers

The technology of containerization is not exclusive to microservices architectures, but the concepts work well together. Containers are a way to encapsulate application code and its dependencies so that they can be deployed effortlessly in any platform.

Traditional application deployments require the organization to install software first, such as the application runtime, programming libraries, or external components. This approach often results in the "it works on my machine" problem: it's difficult to replicate the same environment across development, test, staging, and production. Small differences in the way that the application dependencies are installed can cause the application to work fine while being tested, but fail when it's deployed into production.

Containers change the game rules. The application dependencies are packed along with the application code in an autonomous deployment unit, the container image. Whether the application container is deployed on a developer's laptop or in a production cluster with hundreds of nodes, the dependency handling is the same. The container will work exactly the same way, so application testing is more reliable and trustworthy.

Containers have come a long way since Docker released their code as open source in 2013. Containers support now both Linux and Windows, and different CPU architectures such as ARM. There are many offers in Azure that allow container-based workloads to run. In this unit, you'll learn some of them.

Kubernetes and Red Hat OpenShift

A container runtime is the technology that starts containers on a computer, but more logic is required in a production environment. Who will deploy more containers, if more performance is required? Who will restart the containers if they have a problem? If multiple computers are available, who will decide on which of them a certain container should be started? These and other tasks are the responsibility of a container orchestration platform.

The first version of Kubernetes was released in 2015, and it soon became the *de facto* standard for container orchestration. Kubernetes clusters consist of several worker nodes. Each worker node has a container runtime, so it can run containers where the Kubernetes control plane will schedule the deployment of containerized applications. This control plane typically runs in a set of master nodes. It's responsible for keeping the application running correctly, scaling the application up or down, and carrying out any required updates.

One of the main reasons for the popularity of Kubernetes is the hardware independence that containers provide. Because container-based applications can be reliably deployed to any container runtime, you can run Kubernetes in clouds that use various hypervisors. The deployed applications should behave in a similar way (assuming that the underlying hardware resources are similar too). Many organizations have adopted Kubernetes as an abstraction layer that allows consistent application deployment processes both on-premises and in public clouds.

Running Kubernetes in Azure is easy. Azure Kubernetes Service is simple to deploy and cost efficient, because the customer is only charged for the cost for the worker nodes. Microsoft carries the cost and operation of the master nodes. Microsoft will patch and update the operating system of the worker nodes, further reducing the operational complexity of managing a Kubernetes cluster to run Linux and Windows containers.

OpenShift is an application-deployment platform based on Kubernetes. It incorporates many other functionalities and is developed and supported by Red Hat. Some of the organizations that choose to run their applications on OpenShift do so because of these extra features and the support that Red Hat provides. Running OpenShift on Azure is again simple. Azure Red Hat OpenShift consists of an OpenShift cluster where many of its aspects are managed by Microsoft, including the whole lifecycle of the cluster.

Azure App Service

Azure App Service is a platform where organizations can run their web-based workloads without having to manage any orchestrator or underlying operating system. The only requirement is uploading the application code to the service through one of many available deployment methods. Azure will do the rest: scaling the application in and out, patching and maintaining the underlying virtual machines, and much more, without requiring the learning curve of Kubernetes.

Azure App Service supports container-based workloads, so you can upload your container image instead of the application code. It also supports Linux and Windows workloads, and many different application runtimes.

Azure App Service supports various pricing models, including a serverless option called Azure Functions. In Azure Functions, only application usage is charged. There are no fixed costs.

The serverless model is interesting for innovating, because it allows deploying new microservices without incurring high monthly bills if the market doesn't accept them. This is another example of the fail-fast strategy, where innovation does not necessarily mean high expenses.

Azure App Service also offers features that support DevOps-oriented deployments, such as web app slots. Slots are staging areas where you can deploy new features without affecting the production environment. This is great from an innovation perspective, because you can redirect a small selection of your customers to this new version of the application and then validate whether your innovation hypothesis is correct. Eventually, if you want to promote the new code to production, you can "swap" slots so that the staging environment becomes the production version.

Summary

In this unit, you learned how technology can support innovation:

- DevOps processes and tools will give your development and operations teams the superpower of delivering new features quickly and reliably.
- Applications can be rearchitected into microservices to allow innovating on their components individually, without affecting the rest.
- Containers enable reliable application deployment across multiple platforms and environments.
- Kubernetes is a cloud-agnostic orchestration platform to run containerized applications.
- Azure App Service can run web-based workloads with minimum management overhead. It offers many features, like serverless or application slots, to speed up the innovation cycle.

Tailwind Traders has decided to start the redesign of its e-commerce application into a microservices architecture. The first application subsystem that it will separate from the "monolith" is the payment service, because this has been identified as a critical area where the competition is offering better value to customers.

After the payment subsystem, more application components will be converted into independent microservices. The microservices will communicate through REST APIs. The application code for each microservice will be containerized, and the development and operations organizations will adopt DevOps best practices.

Because Tailwind Traders doesn't want to be dependent on any specific public cloud, it has decided to build Kubernetes expertise in-house and deploy the application on Azure Kubernetes Service clusters. If new microservices need to be developed, the company will consider Azure Functions as a platform for MVP deployment to reduce development costs.

Where to look next

Many of the concepts in this unit are further articulated in the Cloud Adoption Framework articles Empower adoption with digital invention and Kubernetes in the Cloud Adoption Framework.

Next unit: Infuse your applications with AI

Continue >

100 XP

Infuse your applications with AI

9 minutes

In this unit, you'll learn the importance of machine learning and AI technologies in the innovation process and customer experience.

Machine learning and AI to create value

When you're evaluating which application features will enhance the user experience and increase business value, machine learning and AI are great assets to improve the interaction with your customers and partners.

In addition to the transformation of its main e-commerce applications into a microservices architecture, Tailwind Traders is evaluating the introduction of new functionality that enhances the customer experience. Tailwind Traders has no data-science skills. New staff will be hired in the future, but in the meantime, the company should identify quick wins that can help in improving the competitiveness of its web shop.

Tailwind Traders is evaluating four possibilities:

- Embed a recommendation engine to increase cross-sales
- Include a support chat to improve the user experience when problems arise
- Redesign the search engine to shorten the time it takes for customers to find products
- Analyze product reviews to better understand customers' sentiments

Tailwind Traders needs to evaluate which Azure technologies can help the company start its journey into infusing its applications with machine learning and AI.

Machine Learning and AI in Azure

Azure offers tools and services that can help organizations build machine learning and AI functionality in applications quicker and at a lower cost.

Azure Cognitive Services

Azure Cognitive Services contains prebuilt models that don't require machine-learning expertise to introduce AI functionality to an application. Azure Cognitive Services encompasses many areas, such as vision, speech, language, decision, and search. It's easy to use, so organizations can use the power of AI without extensive machine-learning skills.

Tailwind Traders sees a high potential in Azure Cognitive Services, because its data-science department is not fully operational. The company will evaluate these features to innovate the e-commerce application:

- **Personalizer**: Organizations can use this feature to learn which users prefer which products, and to make fine-tuned, individual recommendations. Some customers prefer products with quick delivery, whereas other customers prefer products on sale. Personalizer uses a type of machine learning algorithm called *reinforcement learning*, which doesn't require huge amounts of data to be trained. This is interesting for Tailwind Traders, because the data doesn't exist yet.
- **Text Analytics**: Many users write product reviews. Organizations can analyze reviews to find customers who express negative sentiments. Focusing on these customers can reduce customer churn and increase loyalty.
- **Translator**: Product reviews can be an effective sales tool, but they're useful only to customers who understand the language they're written in. Using real-time translation services would allow Tailwind Traders to show product reviews to any user regardless of their native language.

Other Azure Cognitive Services features have potential for Tailwind Traders, but the company decided to start with the previous three. The reason is the positive ratio between the potential increase in business impact and the low effort that their introduction would require.

Knowledge mining and Azure Cognitive Search

Azure Cognitive Search helps introduce knowledge mining and flexible search engines into applications with little coding effort. Not only can the service index massive amounts of data, it can also add enrichments to augment the information available to search.

One of the areas where the Tailwind Traders application needs to be improved is the product search. Customers spend too much time trying to find the product they're looking for. Replacing the existing search engine with Azure Cognitive Search will allow the company to expose rich search controls such as faceted navigation (multiple-category filters), relevance tuning, and autocomplete.

Internet users are used to sophisticated search engines, so Tailwind Traders can't afford to continue offering the old-fashioned functionality in the present version of the e-commerce

platform. Fortunately, Azure Cognitive Search is offered as a set of APIs that enable the quick creation of MVPs.

Azure Bot Service

The next area where surveys have surfaced user dissatisfaction is customer support. Long resolution times and congested phone lines are common complaints.

Tailwind Traders is considering Azure Bot Service to implement a chat-based support system where users can resolve their issues quicker at a lower cost. Azure Bot Service can be implemented in various languages, like C#, JavaScript, and Python. This makes it easier to find developers in the organization who can use a familiar programming language to create the chat functionality.

Azure Bot Service can be implemented in various channels, but Tailwind Traders is mostly interested in offering it as a web-based chat for users who visit the e-commerce website.

Azure Machine Learning

Azure Machine Learning facilitates the process of creating custom machine-learning models, deploying those models to production, and managing versions of all deployed models across the organization.

Azure Machine Learning makes the job of data scientists easier by helping them to share experiment results and manage different models at scale. It can refine models with hyperparameter tuning, and even create new ones with automated learning. It can then deploy the selected models to Kubernetes clusters to offer highly scalable, enterprise-grade APIs that will run the organization's machine-learning models in production.

Tailwind Traders is considering using custom models for a next-generation product recommender that would be more sophisticated than the Recommender feature in Azure Cognitive Services. However, this improvement will be possible only when data-science expertise exists in the organization.

Tailwind Traders analysis

Tailwind Traders has formulated the hypothesis "A recommendation engine would increase cross-sales." Ideally, Tailwind Traders would use the Azure Machine Learning service to build a recommendation engine that's tailored to the organization's needs. However, the company has no data-science expertise at the moment.

For now, Tailwind Traders has decided to use the Personalizer feature in Azure Cognitive Services to enrich the application without the need for data scientists. If the hypothesis is validated, the data science team that's eventually hired will evolve the prototype with custom machine-learning models built with Azure. An example is in the article Build a real-time Recommendation API on Azure.

Additionally, Tailwind Traders has decided to validate the existing hypothesis around building a support chat with Azure Bot Service and improving the e-commerce site with Azure Cognitive Search. Both prototypes can be built with relatively low effort, so Tailwind Traders can start its foray into machine learning and AI at full speed.

Next unit: Azure technologies for measuring business impact

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Azure technologies for measuring business impact

8 minutes

After an organization builds an MVP, it needs to validate the innovation hypothesis. In this unit, you'll learn how Azure tools can help in this crucial part of the innovation process.

Measuring effectiveness

Measuring whether a hypothesis was right or wrong can be tricky, because multiple factors might be influencing key performance indicators. These factors might give hints about the expected success, because establishing causality can be complex. For example, even if sales increase after the introduction of a certain feature, whether the new feature was the main factor responsible for the sales increase is hard to prove.

However, the way in which features are released to application users can help to assess the validity of a hypothesis:

- Controlled deployments with *feature flags*, *feature rings*, and *canary deployments* allow you to release a feature to a limited set of users to prevent disrupting the experience of the whole customer base. Additionally, you can directly compare the performance of the customers with and without the feature to each other.
- *Portal options* for users to decide if they want to be exposed to new functionality puts the users in control of their own experience. The fact that many users opt for a new feature might already be a confirmation that the previous functionality had room for improvement. If customers that had opted for the new feature go back to the previous experience, that might be an indicator that the deployed MVP is missing the mark.
- *Customer surveys* are a powerful feedback mechanism, if they're implemented correctly. Customers will provide information about their satisfaction if it's simple to give. One-click "traffic light" satisfaction surveys or single questions about new functionality might provide insights to help in evaluating whether the innovation hypothesis was correct. In general, only a few users will answer longer surveys and will take the time to fill them in thoroughly and truthfully.

Understanding your application

Understanding your application

Azure Application Insights is an application performance management (APM) platform with a rich set of tools to gather application telemetry for multiple purposes, such as performance monitoring, problem troubleshooting, or understanding how users move through applications. The last item is critical for the innovation lifecycle, because it can be used to validate an innovation hypothesis and to judge whether a certain innovation is improving the customer experience.

Detect problems before users do

A crucial element that affects the user experience is the performance and availability of an application. If an application is not working correctly and running into errors, or if it's not responsive enough, some users will abandon it out of frustration. Your organization might lose business. Those frustrated users might also damage your organization's reputation if they share their experience on social media.

Detecting those problematic situations before they affect users is of the highest importance. To meet that goal, you need to proactively monitor the application and start working on potential problems before they affect the business. For example, you can enable notifications to automatically open incidents so that they're investigated before customers report them.

Smart Detection is a useful feature of Azure Application Insights. It can raise alerts when the application behavior is unusual. It detects anomalies by using machine learning, and the alerts are richer than traditional error notifications.

Notifications typically report that there might be a problem, without context about the potential business impact. Smart Detection alerts include information like the number of affected users, the pattern associated with the failures, or the failure rate compared to normal behavior. You can then focus on the most critical issue from a business perspective.

Monitor user activity

Usage analysis in Azure Application Insights can help you evaluate which application areas need to be improved. For example, usage analysis can identify the most popular application features or specific points at which users leave the web portal. You can explore, for example, whether your application works better in certain geographic areas than others, to get valuable information about where the application gaps might be.

After you formulate a hypothesis with the data provided by Azure Application Insights, you can analyze telemetry to measure whether the situation is now better or worse. Custom

business events can be embedded in the application so that telemetry data contains

additional information that will help in the measure process.

Funnels can be an insightful tool. With funnels, you can predefine expected *flows* that users will follow when they use the application. This allows you to monitor which patterns users follow. You can then identify problems in the applications if users are behaving in unexpected ways.

Retain users

The Application Insights retention tool offers specific functionality around user churn. Combined with business events, it contains valuable learning data. For example, understanding which actions were taken by customers who left the application unexpectedly will allow you to formulate hypotheses with maximum business impact.

For example, if most users who abandoned your website did so from the payment method page, you would suspect a business problem there. Maybe the payment options are insufficient or not clearly displayed. Or another problem is preventing users from moving forward in their shopping process.

Impact analysis

Impact analysis is a feature in Azure Application Insights that correlates technical aspects of the application to tangible business metrics.

For example, how fast should the product page load so that most users continue with their shopping process? With impact analysis, you can show the relationship between page load time and the rate of users who purchase the product shown. This information can help you to validate or reject an innovation hypothesis, and to convert business requirements into technical specifications.

Summary

Tailwind Traders decided to introduce some new features in its e-commerce application, such as a new payment platform. The application has been instrumented with Azure Application Insights to understand how many customers are using the new payment method, and whether there's an increase of conversion rate in the payment process. The new payment method was marked as a preview, so that users would be more understanding if there were problems.

Application Insights helped Tailwind Traders to identify that a high percentage of users decided to pick up the new payment method in spite of the "preview" banner. Application

Insights confirmed that the new functionality worked as expected without major flaws.

Additionally, the purchase conversion rate increased significantly.

Tailwind Traders can now focus on turning the MVP for the new payment method into a production-grade feature. The company can move to the learn phase of the innovation lifecycle, to formulate more hypotheses.

Next unit: Azure technologies for the learn process

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Azure technologies for the learn process

8 minutes

In this unit, you'll learn how to apply the results of the measure step in the innovation lifecycle, and the importance of data democratization.

Data democratization

As you've learned in previous units, you can collect data from your customers by using multiple sources. These sources include micro surveys, utilization data derived by Azure Application Insights, and feature flags that customers can decide on their own to enable or disable. The more data you have, the better your decisions will be, but you need a way to handle this ever-increasing flow of data.

In 2014, Satya Nadella talked about the importance of the data culture in an organization. He said that decisions shouldn't be made based on feelings or subjective opinions, but by using data to validate them. He also said that data should be available to every individual who needs it, and it should be easily converted into actionable insights to facilitate data-driven decisions.

An organization can make pervasive data decisions only if those decisions are based on a solid, accessible data platform. This effort involves four areas:

- **Collect data**: The first step to data-driven decision making is always having data. Data collection can take multiple forms: migration from existing data repositories, data generation from sources like Azure Application Insights, or data ingestion from other sources.
- **Share data**: Collected data needs to be available to everybody who needs it, not only to data experts. All individuals in an organization should be able to use data to make their decisions.
- **Centralize data**: Centralized data platforms can help to simplify data sharing and governance.
- **Govern data**: Data sharing does not mean that all data needs to be available to everybody. Ensure that any sensitive data is secured, tracked, and governed before sharing it.

Azure data platform

The Azure platform covers the whole data lifecycle, which is fundamental for data-driven decision making and data democratization. From lightweight, on-demand databases to massive data warehouses or flexible NoSQL systems, the Azure data platform allows you to cover the four data activity areas.

Data collection

The Azure data ecosystem includes services and tools to migrate, ingest, store, and analyze data. The following list shows only a few of the mechanisms that you can use to process data and make it available for later sharing, in order to facilitate data-driven decision making:

- **Data analytics**: Azure Synapse Analytics is an enterprise analytics service that accelerates time-to-insight across data warehouses and big-data systems. Azure Synapse Analytics brings together the best of:
  - SQL technologies used in enterprise data warehousing
  - Spark technologies used for big data
  - Pipelines for data integration and ETL (extract, transform, load) and ELT (extract, load, transform)
  - Deep integration with other Microsoft services such as Power BI, Azure Cosmos DB, and Azure Machine Learning
- **Data migration**: Data might be already stored in existing sources, but it needs to be migrated to a modern platform before it can be converted into actionable insights. Azure Database Migration Service contains tooling that helps with data migrations from systems such as SQL Server, PostgreSQL, Oracle, and MongoDB.
- **Data processing**: Azure includes services to analyze and transform data streams with Azure Stream Analytics, and to run ETL processes at large scale with Azure Data Factory.

Data sharing

Microsoft Power BI is a set of tools that consolidate data coming from disparate sources into integrated, interactive visualizations. Users can dive into the data just by operating intuitive controls. The power of insights is available to everybody in an organization, not just to data professionals.

Area owners can create reports and dashboards that contain the relevant information around specific aspects of the application. After new functionality is introduced to validate a hypothesis, data is readily available to either validate or reject the hypothesis based on real customer usage.

Microsoft Power BI can help with data sharing from multiple perspectives. Here some examples:

- **Share data with coworkers and partners**: Power BI dashboards simplify consuming data. Visualizations allow for people who aren't data experts to drill down into data without having to be familiar with its underlying structure.
- **Quickly generate data insights**: Power BI can automatically generate visualizations of data sets with its Quick Insights functionality. You can create dashboards quickly and find data correlations that might not have been obvious at first.
- **Embed reports in a website or portal**: With Power BI, not only can visualizations be accessed in the native Power BI portal, but reports and dashboards can be embedded in other web applications too. This way, users don't need to leave their familiar corporate websites to find the data that they need for their decision-making process.

Data centralization

The main problem of data centralization is scale at different levels. At the risk of oversimplifying, it can be reduced to the three "V's" of big data:

- **Volume**: Azure Data Lake Storage Gen2 is a cost-effective and scalable Azure platform for data storage. Based on the massive scalability provided by Azure Storage, Azure Data Lake Storage has been designed to service multiple petabytes of information while sustaining hundreds of gigabits of throughput.
- **Variety**: This term often refers to the fact that data is not always structured. You might have semi-structured and even unstructured data, too. Azure Synapse shines in this area, because it brings together the best of SQL technologies used in enterprise data warehousing with Spark, which is often used for big data.
- **Velocity**: A problem often found in older data architectures is the interdependency between storage capacity, analysis speed, and ingestion rates. In Azure data solutions, an organization can scale different dimensions of the platform independently by decoupling them. Data can be ingested, processed, and shared through data pipelines that use the required Azure data services, as the enterprise business intelligence architecture shows.

Data governance

In today's world, data represents both a critical asset and a significant responsibility. Stored data often includes confidential information that can result in financial or personal damage if it's leaked or shared inappropriately. Storing and processing data implicitly means accepting that responsibility. Legal regulations can result in penalties for organizations that mishandle personal or confidential data.

As a consequence, data governance is critical for any organization that has a goal of data democratization. The first step toward data governance is classifying data that needs to be treated in specific ways. As an example, Microsoft uses these data categories internally for data classification:

- **Non-business**: Data from your personal life that doesn't belong to Microsoft
- **Public**: Business data that's freely available and approved for public consumption
- **General**: Business data that isn't meant for a public audience
- **Confidential**: Business data that can cause harm to Microsoft if overshared
- **Highly confidential**: Business data that would cause extensive harm to Microsoft if overshared

The next step after data classification is ensuring that each data category is protected from unauthorized access. Azure supports these technologies that enforce confidentiality:

- **Encryption of data at rest**: All Azure data is encrypted when stored in Microsoft datacenters. Some Azure services offer specific encryption features, such as transparent data encryption in Azure Synapse and Azure SQL Database.
- **Encryption of data in flight**: All Azure data services encrypt data with SSL or TLS before sending it through the network. Some services, such as Azure Storage, can optionally allow unencrypted traffic. Organizations should disable any unencrypted communication for any type of sensitive data.
- **Data access control**: Azure offers sophisticated authentication and authorization mechanisms both for access to the Azure platform and for access to data itself. Azure role-based access control, Conditional Access, and Privileged Identity Management are three examples of essential services that can help to ensure that only authorized people have access to sensitive information.
- **Data auditing**: Many regulatory compliance standards demand evidence of data protection mechanisms by documenting who has done certain operations and accessed certain data. As described in Auditing for Azure SQL Database and Azure Synapse Analytics, data auditing in Azure contemplates three aspects of auditing:
  - *Retain* an audit trail of selected events, where you can define categories of data actions to be audited
  - *Report* on database activity, optionally with preconfigured reports and dashboards to get started quickly
  - *Analyze* reports to uncover suspicious events, unusual activity, and trends

Growth mindset

The learn phase sometimes delivers bad news. Hypotheses that you thought were right might turn out to be wrong. Being open to alternative ideas is key for the innovation process to flow

smoothly. Maybe the whole hypothesis was wrong, or maybe the problem was only the way in which the prototype was developed.

In any case, conclusions should always be backed by data. The team should move on to formulating the next hypothesis, possibly some kind of revision or iteration of the initial one.

Existing data might not allow you to unequivocally conclude whether the hypothesis was right or wrong. In this case, the data set that's helping the decision process should be enhanced. Either introduce new telemetry points in the application, or figure out new ways of getting information about the customer experience.

A growth mindset is fundamental at this stage. Think of hypotheses proven wrong or partially wrong as learning opportunities. Organizations shouldn't waste time on an innovation that doesn't generate the expected business outcomes.

Where to look next

Many of the concepts in this unit are further discussed in the Cloud Adoption Framework documentation about data democratization.

Next unit: Knowledge check

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

Knowledge check

10 minutes

Check your knowledge

1. What are the main phases of the innovation lifecycle?

- ○ The waterfall process
- ◉ Build, measure, learn

  ✔ **This iterative process is the basic framework to run progressive innovations.**
- ○ Crawl, walk, run

2. Why are microservices architectures often associated with innovation?

- ○ Because microservices architectures are more secure than monolithic software
- ◉ Because they're based in Kubernetes

  ✘ **Although microservices architectures are often based in containerized software, it isn't a requirement.**
- ○ Because they enable introducing new functionality in one microservice without affecting the rest

  ✔ **The ability to innovate on one microservice without having to touch the rest means that new functionality can be implemented quickly.**

3. Why is adopting a DevOps culture critical to enable effective innovation?

- ○ Because it enables testing in production
- ◉ Because it uses GitHub

  ✘ **Although GitHub is a great tool to support your DevOps process, it's not the most important criterion in adopting a DevOps culture in an organization.**

- ○ Because it enables bringing new functionality to applications both quickly and reliably

✔ **Deploying new features quickly and reliably allows you to validate or reject innovation hypotheses faster and more efficiently.**

4. Is Kubernetes a requirement to innovate an application?

- ○ No, but containerization can make the build step faster.

✔ **Application containerization isn't essential for innovation. But it can ease testing and validation of new application code. As a consequence, it accelerates the innovation process.**

- ◉ Yes, only containerized applications can be innovated.

✘ **Although containerization does ease testing and validation of new application code, non-containerized code can be innovated as well.**

- ○ No, because Kubernetes increases the operational complexity for an application.

5. Is it possible to build machine learning and AI into an application without data scientists?

- ○ Yes, with Azure Kubernetes Service.
- ○ Yes, with prebuilt models such as Azure Cognitive Services.

✔ **Azure Cognitive Services has prebuilt APIs ready to be embedded into any application without requiring data science skills.**

- ◉ No, a data science department is always required.

✘ **Although it's true that data scientists can build powerful models adapted to each organization's needs, there are other options if no data science expertise is available.**

6. Which Azure service allows the extraction of telemetry information from user activity to validate or reject innovation hypotheses?

- ○ Azure DevOps
- ○ Azure App Service
- ◉ Azure Application Insights

✔ **Azure Application Insights can track how customers use an application, track how the application performs, and detect anomalies in application performance.**

7. Why is data democratization critical for innovation?

- ○ Because everybody can use spreadsheets
- ◉ Because hypothesis validation should be data driven

  ✔ **Ideally, all decisions in an organization should be driven by data, including the innovation process.**

- ○ Because machine learning is the future

Next unit: Summary

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Summary

3 minutes

In this module, you learned how Azure technologies can support you along the innovation cycle (build, measure, and learn):

- DevOps practices and modern application technologies reduce the duration of loops in the innovation cycle, to accelerate the creation of business value.
- You can use data obtained from the application to analyze whether innovation hypotheses are correct, partially correct, or false. This data also allows you to correlate technical aspects of the application to business metrics.
- Data democratization makes sure that the collected data is used to learn from the innovation cycle, and that a growth mindset culture spreads across your organization.

Tailwind Traders is using Azure to power its innovation engine in multiple ways:

- Azure DevOps allows Tailwind Traders to introduce application changes frequently and reliably.
- The e-commerce platform will be re-engineered into a microservices architecture to facilitate introducing changes.
- Tailwind Traders will containerize the microservices of the e-commerce platform and deploy them on Azure Kubernetes Service.
- Tailwind Traders decided to use Azure machine learning and AI technologies to enrich its applications with a chat for customers to open support cases, a modern product search portal, and a recommendation engine that suggests additional offers to registered users.
- The e-commerce website has been equipped with Azure Application Insights telemetry, which allows Tailwind Traders to gather data on the utilization of new features to confirm or reject hypotheses about the business value that each innovation adds.
- Tailwind Traders chose Microsoft Power BI to disseminate data across its organization. The goal is to ensure that decisions are data driven and that a growth mindset becomes pervasive. This data-driven decision process allows Tailwind Traders to formulate, build, and verify innovation hypotheses quickly to continue improving its customer experience and business impact.

Next steps

For more information about the topics described in this module, read the Cloud innovation in the Cloud Adoption Framework documentation.

100 XP

Introduction

2 minutes

Security is a core consideration for all customers, in every environment. Moving to the cloud is a significant change that requires a shift in your security mindset and approach.

Cloud security is also an ongoing journey of incremental progress and maturity. New services and features are released daily in Azure. Developers rapidly publish new cloud applications built on these services. But attackers are always seeking new ways to exploit misconfigured resources.

How do you keep up and make sure that your cloud deployments are secure? This module examines best practices in cloud security.

Next unit: Customer narrative

Continue

100 XP

Customer narrative

5 minutes

In earlier Learn modules for the Microsoft Cloud Adoption Framework for Azure, we shared the narrative of Tailwind Traders. This module is the next step toward Tailwind's cloud adoption journey. The Tailwind team is evaluating its security posture.

The Tailwind Traders innovation team is rapidly deploying new products and services and migrating out of their data centers. The company's chief information security officer (CISO) is concerned that the company's risk profile is growing quickly and has become larger than originally anticipated. The company hasn't encountered a breach, but now that adoption is ramping up quickly it's a possibility.

Tailwind Traders previously completed the Ready methodology of the Microsoft Cloud Adoption Framework for Azure module. But the company wants to be proactive to prevent future security issues. It also wants to operationalize security practices across its portfolio to improve its overall security posture. As pointed out in previous Tailwind Traders narratives, the company chose a "start small" implementation of Azure landing zones. As a result, it doesn't have all the rich security tools that come with the Azure landing zone accelerator.

> **Note**
>
> If Tailwind Traders had deployed Azure landing zones at an enterprise scale from the beginning, it would already have many of these tools in place. Having the tools would accelerate the company's security journey.

The CISO wants to add proper layers of protection to reduce risk and prepare for inevitable breach situations. For example, the CISO wants to:

- **Reduce risk from major incidents.** The CISO wants to prevent as many incidents as possible, limit the damage of successful attacks, and rapidly detect, respond to, and recover from incidents. She also wants to be able to restore business processes without paying a ransom.
- **Identify and protect sensitive business data.** The CISO wants to clearly identify what business assets are important to the organization and map those assets into technical assets. She also wants to protect those assets appropriately whether they're structured

data, unstructured data, or any types of applications or systems that enable business-critical processes.

- **Rapidly modernize the existing security program.** The CISO wants to modernize the security program with well-planned initiatives that prioritize quick wins and incremental progress across all security disciplines.
- **Show the company has a strong security posture to build confidence with employees, partners, customers, and stakeholders.** The CISO wants to provide the right level of details on Tailwind Trader's security posture to organization leadership, oversight, and business partners. She wants to carefully balance the ability to provide enough information to build trust while limiting risk from disclosing too much data.
- **Proactively meet regulatory and compliance requirements.** The CISO wants to rapidly discover, understand, meet, and report compliance with external requirements.
- **Reduce the cost and complexity of doing business.** The CISO wants to simplify security processes and reduce friction in business processes from security. Modernizing workloads and applying modern security intelligence, automation, monitoring, and defense approaches will be key to this effort.

Finally, the CISO also wants to:

- Gain insights into the company's security posture that will help build confidence and help the company prioritize what work needs to be done next.
- Empower employees, contractors, and business partners to do their jobs securely from anywhere.
- Ensure monitoring and policy enforcement for all access to the organization's resources with a full end-to-end lifecycle approach.

The CISO has decided to improve the security posture of Tailwind Traders' cloud implementations by adding:

- Tools
- Controls
- Architectures
- Security operations
- Administration practices

Next unit: Methodology

Continue >

200 XP

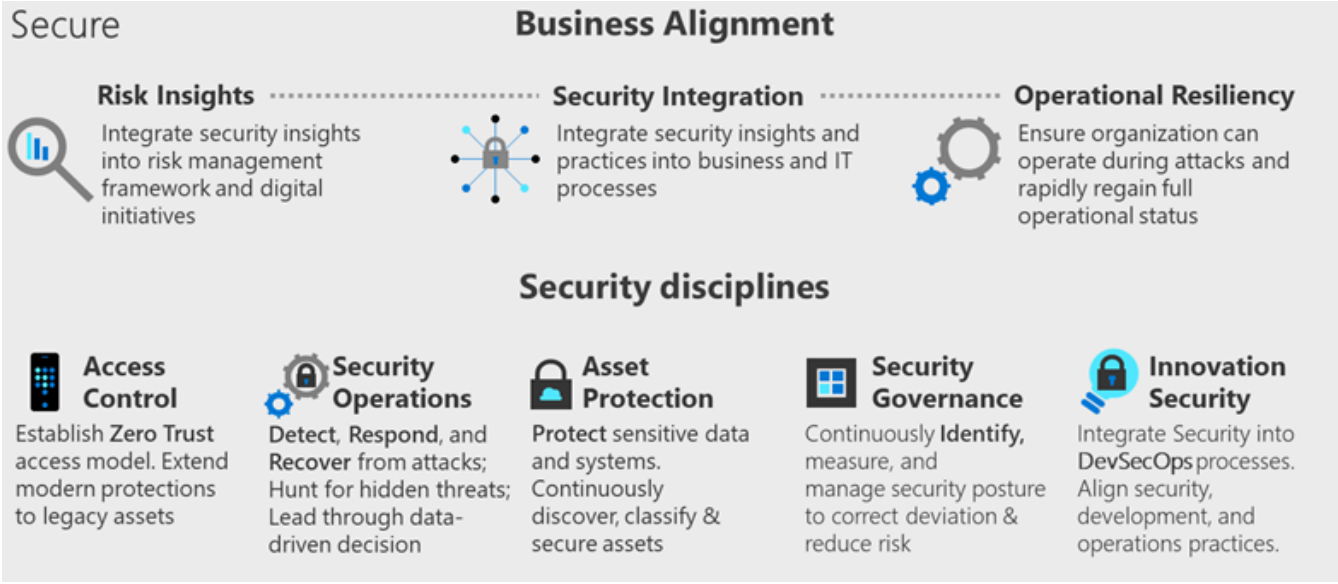
Methodology

5 minutes

The Secure methodology of the Microsoft Cloud Adoption Framework for Azure provides a vision of the complete end state to guide the improvement of your security program over time. The Secure methodology provides a bridge between your business digital transformation and your security program and strategy. It also provides structured guidance for modernizing your security disciplines.

Watch the following video to learn more about the Secure methodology and how it helps guide continuing security improvements over time.

The following infographic provides a visual mapping of the key ways security integrates with the larger organization and the disciplines within security.



Business alignment

Focus your security program on business alignment in three categories:

- **Risk insights**: Align and integrate security insights and risk signals and sources to the business initiatives. Ensure repeatable processes educate all teams on the application of those insights and hold teams accountable for improvements.
- **Security integration**: Integrate security knowledge, skills, and insights deeper into daily operations of the business and IT environment. Use repeatable processes and develop a deep partnership at all levels of the organization.
- **Business resilience**: Prevent as many attacks as possible and limit the damage of those attacks to foster organizational resilience. Ensure that you can continue operations during an attack even if at a degraded state. Also ensure the organization rapidly bounces back to full operations.

Security disciplines

Cloud migration affects each security discipline differently. Each of these disciplines is important and requires continuous investment and improvement as you adopt the cloud:

- **Access control**: Application of network and identity create access boundaries and segmentation to reduce the frequency and reach of any security breaches.
- **Security operations**: Monitor IT operations to detect, respond, and recover from a breach. Use data to continuously reduce risk of breach.
- **Asset protection**: Maximize protection of infrastructure, devices, data, applications, networks, and identities to minimize risk to the overall environment.
- **Security governance**: Monitor decisions, configurations, and data to govern decisions made across the environment and within all workloads across the portfolio.

- **Innovation security**: Integrate security into your DevOps models to improve security and safety assurances as you increase the pace of innovation in your organization. To avoid expensive security incidents and late-stage mitigation, security must become an integral part of a DevSecOps process. Empower workload teams to quickly identify and mitigate security risks.

Check your knowledge

1. Which of the following security disciplines requires continuous investment and continuous improvement as you adopt the cloud?

- ○ Risk insights, security integration, and business resilience.
- ◉ Access control, security operations, asset protection, security governance, and innovation security.

  ✔ **Correct. Each of these areas is extremely important as you adopt the cloud.**

- ○ Monitor decisions, configurations, and data to govern decisions made across the environment and within all workloads across the portfolio.

Next unit: Security roles and responsibilities

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

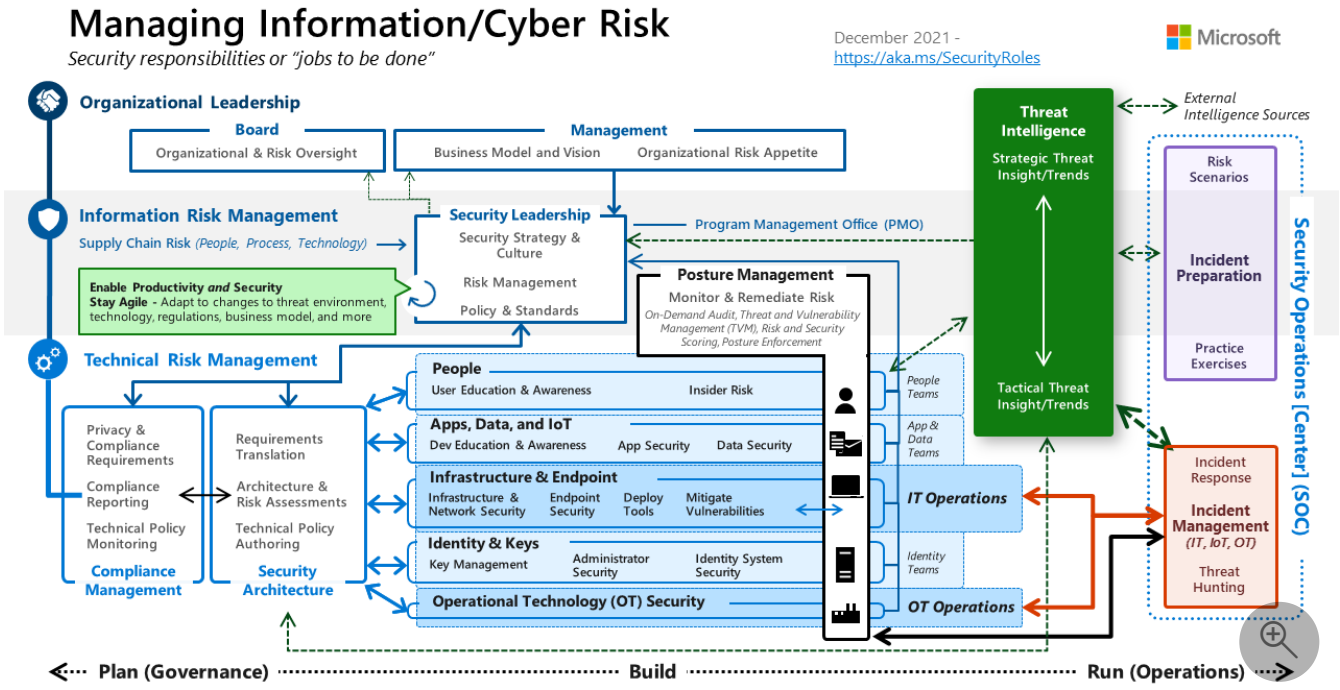
Security roles and responsibilities

10 minutes

Individual security team members must see themselves as part of a security team that's part of the whole organization. They're also part of a larger security community that defends against the same adversaries. This holistic view enables the team to work well in general. It's especially important as teams work through any unplanned gaps and overlaps discovered during the evolution of roles and responsibilities.

Security responsibilities (functions)

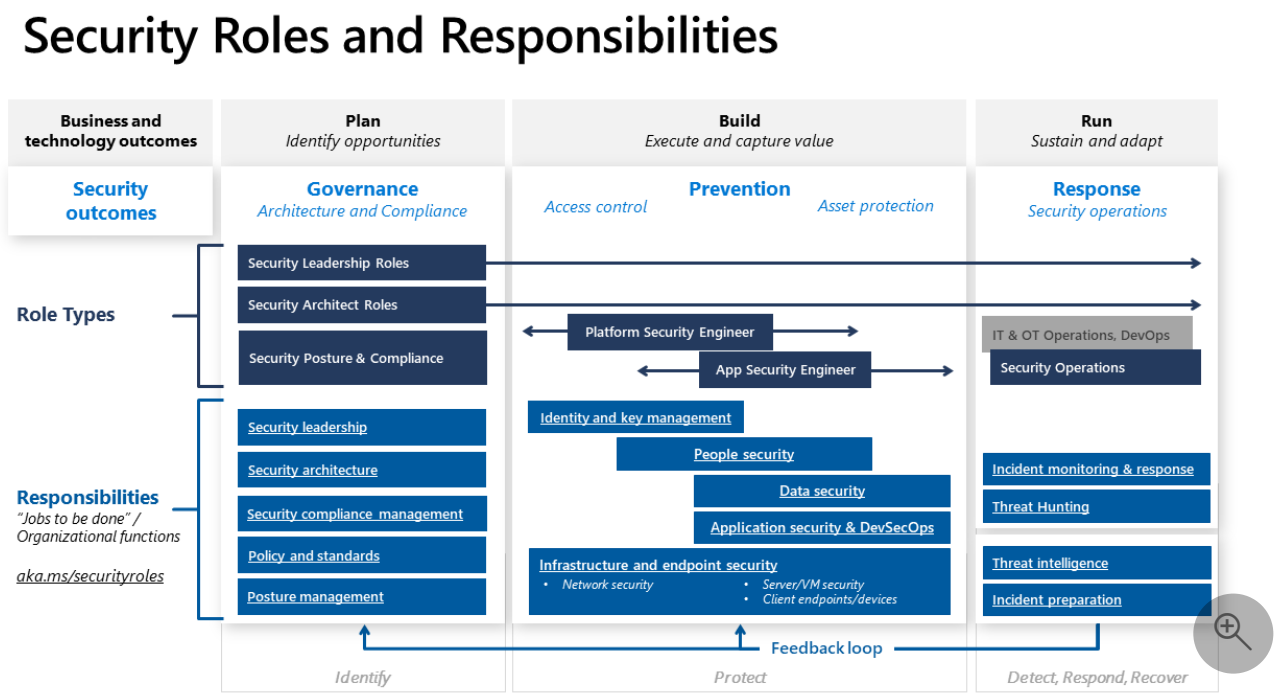
This diagram depicts the specific organizational functions within security. It represents an ideal view of a complete enterprise security team and might be an aspirational view for some security teams. Each function can be performed by one or more people. Each person can perform one or more functions based on factors like culture, budget, and available resources.



The following articles provide information about each function and include a summary of objectives. They discuss how the function can evolve because of the threat environment or cloud technology changes. They also explore the relationships and dependencies that are critical to the function's success:

- Policy and standards
- Security operations
- Security architecture
- Security compliance management
- People security
- Application security and DevSecOps
- Data security
- Infrastructure and endpoint security
- Identity and key management
- Threat intelligence
- Posture management
- Incident preparation

The following diagram summarizes the roles and responsibilities in a security program to help you familiarize yourself with these roles.



For more information, see Cloud security functions.

Map security to business outcomes

At the organizational level, the security disciplines map to standard plan-build-run phases seen widely across industries and organizations. This cycle is accelerating into a continuous change cycle with the digital age and the advent of DevOps. It also illustrates how security maps to normal business processes.

Security is a discipline with its own unique functions. A critical element is integration into normal business operations.

Role types

In the preceding diagram, the dark labels group these responsibilities into typical roles that have common skill sets and career profiles. These groupings also help provide clarity on how industry trends affect security professionals:

- **Security leadership**: These roles frequently span across functions. They ensure that teams coordinate with each other, prioritize, and set cultural norms, policies, and standards for security.
- **Security architect**: These roles span across functions and provide a key governance capability to ensure all the technical functions work harmoniously within a consistent architecture.
- **Security posture and compliance**: This newer role type represents the increasing convergence of compliance reporting with traditional security disciplines like vulnerability management and configuration baselines. While the scope and audience are different for security and compliance reporting, they answer different versions of the question "How secure is the organization?" The way that question is answered is growing more similar via tools like Microsoft Secure Score and Microsoft Defender for Cloud:
  - The use of on-demand data feeds from cloud services reduces the time required to report compliance.
  - The increased scope of data available enables security governance to look beyond traditional software updates or patches and discover and track "vulnerabilities" from security configurations and operational practices.
- **Platform security engineer**: These technology roles focus on platforms that host multiple workloads, focused on access control and asset protection. These roles are often grouped into teams with specialized technical skill sets. They include network security, infrastructure and endpoints, and identity and key management. These teams work on preventive controls and detective controls, with detective controls being a partnership with SecOps and preventive controls being primarily a partnership with IT operations. For more information, see Security integration.
- **Application security engineer**: These technology roles focus on security controls for specific workloads and support classic development models and modern DevOps/DevSecOps model. They blend application and development security skills for unique code and infrastructure skills for common technical components like VMs, databases, and containers. These roles might be in central IT or security organizations or within business and development teams based on organizational factors.

Modernization

Security architecture is affected by different factors:

- **Continuous engagement model**: Continuous release of software updates and cloud features makes fixed engagement models obsolete. Architects should be engaged with all teams working in technical topic areas to guide decision making along those teams' capability lifecycles.
- **Security from the cloud**: Incorporate security capabilities from the cloud to reduce enablement time and ongoing maintenance costs like hardware, software, time, and effort.
- **Security of the cloud**: Ensure coverage of all cloud assets including software as a service (SaaS) applications, infrastructure as a service (IaaS) VMs, and platform as a service (PaaS) applications and services. Include discovery and security of both sanctioned and unsanctioned services.
- **Identity integration**: Security architects should ensure tight alignment with identity teams to help organizations meet the dual goals of enabling productivity and providing security assurances.
- **Integration of internal context in security designs such as context from posture management and incidents investigated by security operations [center]**: Include elements like relative risk scores of user accounts and devices, sensitivity of data, and key security isolation boundaries to actively defend.

Recommended content

- Microsoft Cybersecurity Reference Architectures (MCRA) - People An interactive training guide for people who are new to security.
- MCRA Security Roles - YouTube Overview of the roles and responsibilities in a security program. Includes a discussion of how they're evolving to meet the needs of modern attacks, cloud technology, and Zero Trust principles. This top-to-bottom view of roles includes the board and executives.

Check your knowledge

1. Who's responsible for security in the cloud?

- ○ The CIO/CISO
- ◉ The cloud services provider

❌ **Incorrect. The cloud services provider plays a key role in cloud**

security but isn't solely responsible to maintain the highest levels of security.

- ○ The entire team

  ✔ Correct. It takes effort on the part of every individual within an organization to maintain the highest levels of security.

- ○ The CEO

Next unit: Simplify compliance and security

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

Simplify compliance and security

5 minutes

To speed up implementing the security your organization needs for the cloud, use the Azure Security Benchmark and the landing zones in the Microsoft Cloud Adoption Framework for Azure.

The Azure Security Benchmark represents the recommended practices for security from Microsoft. The Azure Security Benchmark is integrated into the landing zones to simplify the implementation of these best practices.

Security benchmarks

Security benchmarks are configuration baselines and best practices for securely configuring a system. Security benchmarks can help you quickly secure cloud deployments. Benchmark recommendations from your cloud service provider give you a starting point for selecting specific security configuration settings in your environment. Use the settings to quickly reduce risk to your organization.

The Azure Security Benchmark is frequently used to address common challenges for customers or service partners who:

- Are new to Azure and looking for security best practices to ensure a secure deployment of Azure services and application workloads.
- Want to improve the security posture of existing Azure deployments to prioritize top risks and mitigations.
- Need to evaluate the security features and capabilities of Azure services before they onboard and approve an Azure service into the cloud service catalog.
- Must meet compliance requirements in highly regulated industries like government, finance, and healthcare. These customers need to ensure their service configurations of Azure meet strict security specifications. These specifications are defined in frameworks like the:
  - Center for Internet Security (CIS).
  - National Institute of Standards and Technology (NIST).

- Payment Card Industry (PCI).

  The Azure Security Benchmark provides an efficient approach with the controls already pre-mapped to these industry benchmarks.

The Azure Security Benchmark includes high-impact security recommendations to help you secure services you use in Azure. Think of the recommendations as *general* or *organizational* as they apply to most Azure services.

The Azure Security Benchmark recommendations are then customized for each Azure service. The security baselines are the service-specific applications of the benchmark controls. They contain service-level configuration guidance and details.

The Azure Security Benchmark documentation specifies security controls and service recommendations:

- Security controls: The Azure Security Benchmark recommendations are categorized by security controls. Security controls represent high-level vendor-agnostic security requirements, like network security and data protection. Each security control has a set of security recommendations and instructions that help you implement those recommendations.
- **Security baselines**: When available, benchmark recommendations for Azure services include the Azure Security Benchmark recommendations that are tailored specifically for that service.

Implement the Azure Security Benchmark

Implement the Azure Security Benchmark in three steps:

- **Plan your implementation**: Review the documentation for the enterprise controls and service-specific baselines. Plan your control framework and how it maps to guidance like CIS controls, NIST, and the PCI Data Security Standard framework.
- **Monitor your compliance**: Use the Microsoft Defender for Cloud regulatory compliance dashboard to monitor compliance with the Azure Security Benchmark status and other control sets.
- **Establish guardrails**: Automate secure configurations and enforce compliance with the Azure Security Benchmark and other requirements in your organization with Azure Policy.

Check your knowledge

1. What's the purpose of security benchmarks?

- ○ They help you quickly secure cloud deployments and reduce risk to your organization.

  ✔ **Correct. Security benchmarks are configuration baselines and best practices for securely configuring a system.**

- ○ They help you manage workloads in the cloud.
- ◉ They help you migrate specific workloads to the cloud less securely.

  ✘ **Incorrect. The aim of security benchmarks is to help you make your organization more secure.**

- ○ They enable the CISO to offload security responsibilities to the cloud services provider.

Next unit: Simplify security implementation

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

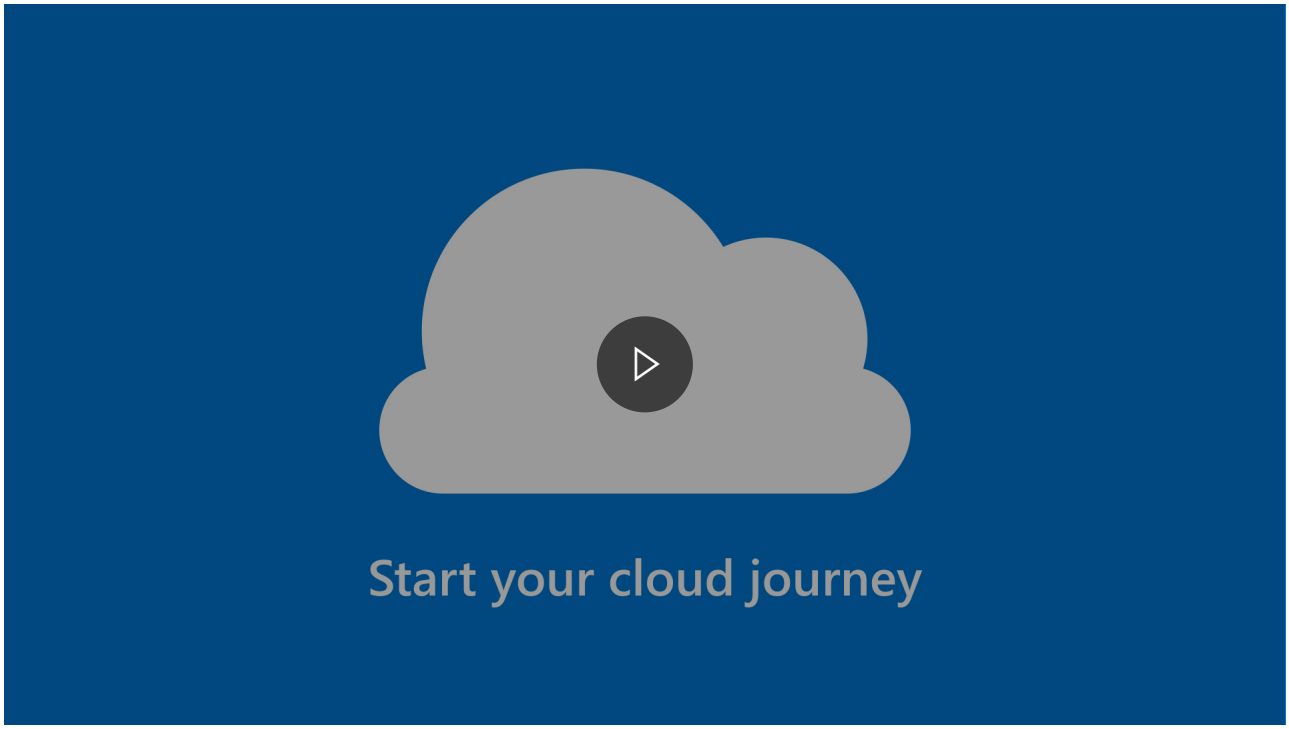
200 XP

Simplify security implementation

5 minutes

Azure landing zones are a logical construct that captures everything that must be true to enable application migrations and development at scale in Azure. Landing zones consider all platform resources that are required to support your organization's application portfolio. Azure landing zones provide cloud adoption teams with a well-managed environment for their workloads.

Landing zones help with cloud adoption by creating better ways to organize resources, not just by type but by organization, cost, and security. Watch the following video.



When you design and implement an Azure landing zone, consider security throughout the process. The security design area focuses on considerations and recommendations for landing zone decisions. Azure Security Benchmarks are built into Azure landing zones to make adopting a strong security stance easier.

The security design area creates a foundation for security across Azure, hybrid, and multicloud environments. The design considerations for security within the Azure landing zones focus on providing visibility into what's happening within the technical cloud estate.

Security monitoring and audit logging of Azure platform services are key components of a scalable framework. The security operations design considerations have in-scope security

alerts, logs, and controls. They also include vulnerability management, shared responsibilities, and encryption and keys. The foundation can later be enhanced with security guidance outlined in the Secure methodology of the Microsoft Cloud Adoption Framework for Azure.

Continue to learn about implementation options for Azure landing zones by reviewing the best practices in the Ready methodology of the Cloud Adoption Framework. Those practices help you to choose how and when to refactor your landing zone to better fit your needs.

Learn how Cloud Adoption Framework enterprise-scale landing zones can help your organization accelerate cloud adoption from months to weeks. See the Create an enterprise-scale architecture in Azure learning path.

Security implementation best practices

Several key steps can help you to mitigate or avoid the business risk from cybersecurity attacks. They can also help you rapidly establish essential security practices in the cloud. Follow the steps to integrate security into your cloud adoption process.

Adhering to these steps helps you integrate security at critical points in the process. The goal is to avoid obstacles in cloud adoption and reduce unnecessary business or operational disruption.

These steps show you how to:

- Establish essential security practices.
- Modernize the security strategy.
- Develop a security plan.
- Secure new workloads.
- Secure existing cloud workloads.
- Govern to manage and improve security posture.

This Get started guide describes the key steps. Use it to help you rapidly establish essential security practices in the cloud and integrate security into your cloud adoption process.

Check your knowledge

1. What's the purpose of Azure landing zones?

○ Landing zones provide a starting point for selecting specific security configuration settings in your environment.

✔ **Correct. Landing zones ensure that when an application or workload lands on Azure, the requisite infrastructure is already in place.**

- ○ Help with cloud adoption by creating better ways to organize resources by type alone.
- ◉ Evaluate relative risk scores of user accounts and devices, sensitivity of data, and key security isolation boundaries to actively defend.

  ✗ **Incorrect. Landing zones don't evaluate risk scores but provide cloud adoption teams with a well-managed environment for their workloads.**
- ○ Help organizations meet the dual goals of enabling productivity and providing security assurances.

Next unit: Security tools and policies

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

200 XP

Security tools and policies

5 minutes

In the Tailwind Traders narrative, the customer chose a "start small" approach to Azure landing zones. This means that their current implementation doesn't include all the suggested security controls. Ideally, the customer would have started with the Azure landing zone accelerator, which would have already installed many of the following tools.

This unit describes which controls to add to this customer's environment to move closer to the Azure landing zones conceptual architecture and prepare the organization's security requirements.

Several tools and controls are available to help you quickly achieve a security baseline:

- Microsoft Defender for Cloud: Provides the tools needed to harden your resources, track your security posture, protect against cyberattacks, and streamline security management.
- Azure Active Directory (Azure AD): The default identity and access management service. Azure AD provides an identity security score to help you assess your identity security posture relative to Microsoft's recommendations.
- Microsoft Sentinel: A cloud-native SIEM that provides intelligent security analytics for your entire enterprise, powered by AI.
- Azure Distributed Denial of Service (DDoS) standard protection plan (optional): Provides enhanced DDoS mitigation features to defend against DDoS attacks.
- Azure Firewall: A cloud-native and intelligent network firewall security service that provides threat protection for your cloud workloads running in Azure.
- Web Application Firewall: A cloud-native service that protects web apps from common web-hacking techniques such as SQL injection and security vulnerabilities such as cross-site scripting.
- Privileged Identity Management (PIM): A service in Azure AD that enables you to manage, control, and monitor access to important resources in your organization.
- Microsoft Intune: A cloud-based service that focuses on mobile device management and mobile application management.

The following sections illustrate how Tailwind Traders might achieve a security baseline in practice.

Baseline implementation for access control

The CISO wants to achieve the following objectives from the customer narrative:

- Allow people to do their jobs securely from anywhere.
- Minimize business damage from a major security incident.

If these objectives align to your organization, or if you have other drivers to increase access controls, factor the following tasks into your security baseline:

- Implement Azure AD to enable strong credentials.
- Add Intune for device security.
- Add PIM for privileged accounts to move closer to a Zero-Trust world.
- Implement sound network segmentation by using a hub-and-spoke model with break-glass controls and firewall controls between application landing zones.
- Add Defender for Cloud and Azure Policy to monitor adherence to these requirements.

Baseline implementation for compliance

The CISO wants to achieve the following objective from the customer narrative:

- Proactively meet regulatory and compliance requirements.

If this objective aligns to your organization, or if you have other drivers to increase access controls, factor the following task into your security baseline:

- Add PIM for privileged accounts to move closer to a Zero-Trust world.

Baseline implementation for identifying and protecting sensitive business data

The CISO wants to achieve the following objectives from the customer narrative:

- Identify and protect sensitive business data.
- Rapidly modernize the existing security program.

If these objectives align to your organization, or if you have other drivers to increase access controls, factor the following tasks into your security baseline:

- Add Defender for Cloud to gain centralized, integrated visibility and control over a sprawling digital footprint and understand what exposures exist.
- Add Microsoft Sentinel to automate processes that are repeatable to free up time for the security team.

After the right tools are in place, make sure you have good policies in place to enforce proper use of those tools. Several policies apply to online and corporate-connected landing zones:

- Enforce secure access, like HTTPS, to storage accounts: Configure your storage account to accept requests from secure connections only by setting the **Secure transfer required** property for the storage account. When you require secure transfer, any requests that originate from an insecure connection are rejected.
- Enforce auditing for Azure SQL Database: Track database events and write them to an audit log in your Azure storage account, Log Analytics workspace, or event hubs.
- Enforce encryption for Azure SQL Database: Transparent data encryption helps protect SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics against the threat of malicious offline activity by encrypting data at rest.
- Prevent IP forwarding: IP forwarding enables the VM a network interface is attached to. You can receive network traffic not destined for one of the IP addresses assigned to any of the IP configurations assigned to the network interface. You can also send network traffic with a different source IP address than the one assigned to one of a network interface's IP configurations. The setting must be enabled for every network interface that's attached to the VM that receives traffic that the VM needs to forward.
- Ensure subnets are associated with network security groups (NSGs): Use an Azure NSG to filter network traffic to and from Azure resources in an Azure virtual network. An NSG contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

Check your knowledge

1. Which of the following is *not* a tool available to help you quickly achieve a security baseline?

- ○ Azure Firewall
- ◉ Azure Web Application Firewall

  ✗ **Incorrect. Azure Web Application Firewall is a cloud-native service that protects web apps from common web-hacking techniques such as SQL injection and security vulnerabilities such as cross-site scripting.**
- ○ Reaper

  ✓ **Correct. Reaper was the first antivirus software created, circa 1972.**
- ○ Microsoft Sentinel