Mustafa Saifee(Microsoft
Student Partner 2015-19)

AZURE FUNDAMENTALS

Apply and monitor infrastructure standards with Azure Policy

-Microsoft Learning

Disclaimer: The information contained in this document is completely owned and published by Microsoft Learning. I claim no credits to any of the content as I have just accumulated the available information for ease of read and learning. This document is/will/should not be used for any revenue systems.

Contents

Introduction

Good IT governance involves planning your initiatives and setting priorities on a strategic level to help manage and prevent issues.

You need good governance when:

- You have multiple engineering teams working in Azure
- You have multiple subscriptions in your tenant
- You have regulatory requirements which must be enforced
- You want to ensure standards are followed for all IT allocated resources

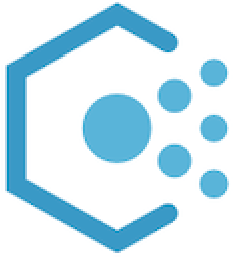
You could enforce standards by not allowing teams to directly create Azure resources - and instead have the IT team define and deploy all cloud-based assets. This is often the solution in on-premises solutions, but this reduces the team agility and ability to innovate. Instead, Azure provides several tools you can use to enforce and validate your standards, while still allowing your engineering teams to create and own their own resources in the cloud.

In addition to providing IT standards, you need to be able to monitor your resources to make sure they are responsive and performing properly. Azure provides several built-in features to track and analyze your resource utilization and performance.

In this module, you will:

- Apply policies to control and audit resource creation
- Learn how role-based security can fine-tune access to your resources
- Understand Microsoft's policies and privacy guarantees
- Learn how to monitor your resources

Define IT compliance with Azure Policy



Planning out a consistent cloud infrastructure starts with setting up policy. Your policies will enforce your rules for created resources, so your infrastructure stays compliant with your corporate standards, cost requirements, and service-level agreements (SLAs) you have with your customers.

Azure Policy is a service in Azure that you use to define, assign, and, manage standards for resources in your environment. It can prevent the creation of disallowed resources, ensure new resources have specific settings applied, and run evaluations of your existing resources to scan for non-compliance.

Azure Policy comes with many built-in policy and initiative definitions that you can use, under categories such as Storage, Networking, Compute, Security Center, and Monitoring.

Imagine we allow anyone in our organization to create virtual machines (VMs). We want to control costs, so the administrator of our Azure tenant defines a policy that prohibits the creation of any VM with more than 4 CPUs. Once the policy is implemented, Azure Policy will stop anyone from creating a new VM outside the list of allowed stock keeping units (SKUs). Also, if you try to *update* an existing VM, it will be checked against policy. Finally, Azure Policy will audit all the existing VMs in our organization to ensure our policy is enforced. It can audit non-compliant resources, alter the resource properties, or stop the resource from being created.

Tip

Azure Policy can integrate with Azure DevOps, by applying any continuous integration and delivery pipeline policies that affect the pre-deployment and post-deployment of your applications.

Creating a policy

The process of creating and implementing an Azure Policy begins with creating a *policy definition*. Every policy definition has conditions under which it is enforced. And, it has an accompanying effect that takes place if the conditions are met. To apply a policy, you will:

1. Create a policy definition
2. Assign a definition to a scope of resources
3. View policy evaluation results

What is a policy definition?

A *policy definition* expresses what to evaluate and what action to take. For example, you could ensure all public websites are secured with HTTPS, prevent a particular storage type from being created, or force a specific version of SQL Server to be used.

Here are some of the most common policy definitions you can apply.

Policy definition	**Description**
Allowed Storage Account SKUs	This policy definition has a set of conditions/rules that determine whether a storage account that is being deployed is within a set of SKU sizes. Its effect is to deny all storage accounts that do not adhere to the set of defined SKU sizes.
Allowed Resource Type	This policy definition has a set of conditions/rules to specify the resource types that your organization can deploy. Its effect is to deny all resources that are not part of this defined list.
Allowed Locations	This policy enables you to restrict the locations that your organization can specify when deploying resources. Its effect is used to enforce your geographic compliance requirements.
Allowed Virtual Machine SKUs	This policy enables you to specify a set of VM SKUs that your organization can deploy.
Not allowed resource types	Prevents a list of resource types from being deployed.

The policy definition itself is represented as a JSON file - you can use one of the pre-defined definitions in the portal or create your own (either modifying an existing one or starting from scratch). There are hundreds of samples available on GitHub.

Here is an example of a Compute policy that only allows specific virtual machine sizes:

JSON

```
{
  "if": {
    "allOf": [
      {
        "field": "type",
        "equals": "Microsoft.Compute/virtualMachines"
      },
      {
        "not": {
          "field": "Microsoft.Compute/virtualMachines/sku.name",
          "in": "[parameters('listOfAllowedSKUs')]"
        }
      }
    ]
  },
  "then": {
    "effect": "Deny"
  }
}
```

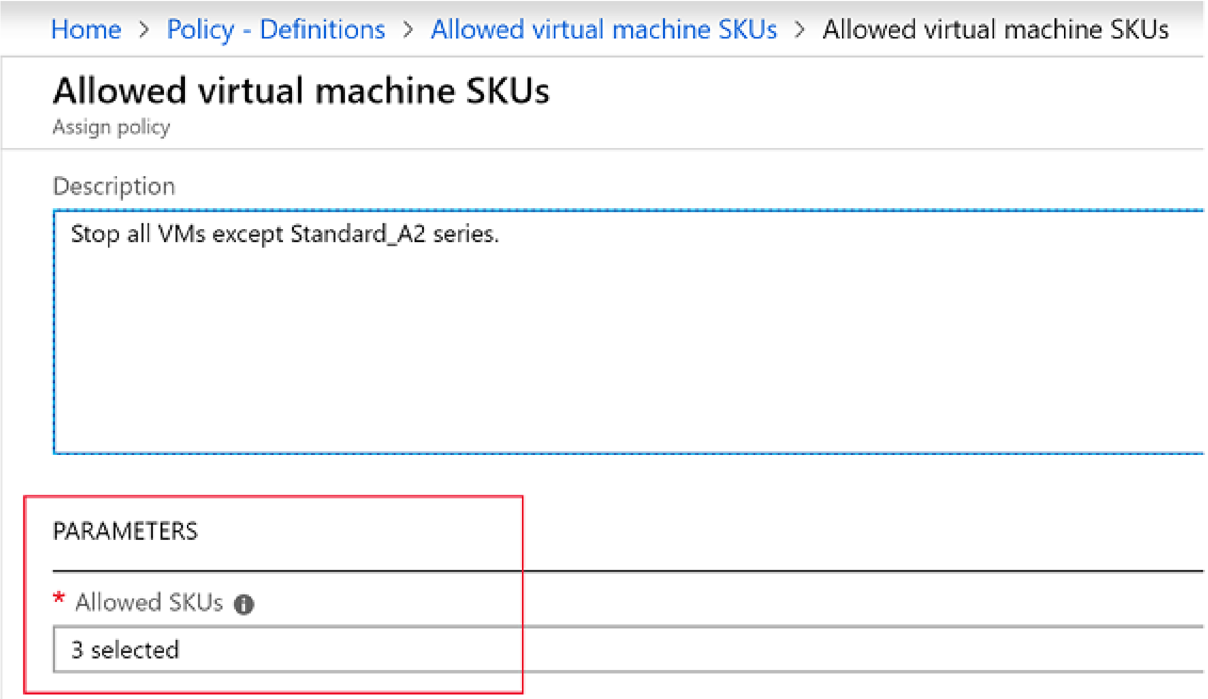
Notice the [parameters('listofAllowedSKUs')] value; this is a replacement token that will be filled in when the policy definition is applied to a scope. When a parameter is defined, it's given a name and optionally given a value.

Assign a definition to a scope of resources

Once you've defined one or more policy definitions, you'll need to assign them. A *policy assignment* is a policy definition that has been assigned to take place within a specific scope.

This scope could range from a full subscription down to a resource group. Policy assignments are inherited by all child resources. This means that if a policy is applied to a resource group, it is applied to all the resources within that resource group. However, you can exclude a subscope from the policy assignment. For example, we could enforce a policy for an entire subscription and then exclude a few select resource groups.

You can assign any of these policies through the Azure portal, PowerShell, or Azure CLI. When you assign a policy definition, you will need to supply any parameters which are defined.


Home > Policy - Definitions > Allowed virtual machine SKUs > Allowed virtual machine SKUs

Allowed virtual machine SKUs
Assign policy

Description: Stop all VMs except Standard_A2 series.

PARAMETERS

* Allowed SKUs: 3 selected

Policy effects

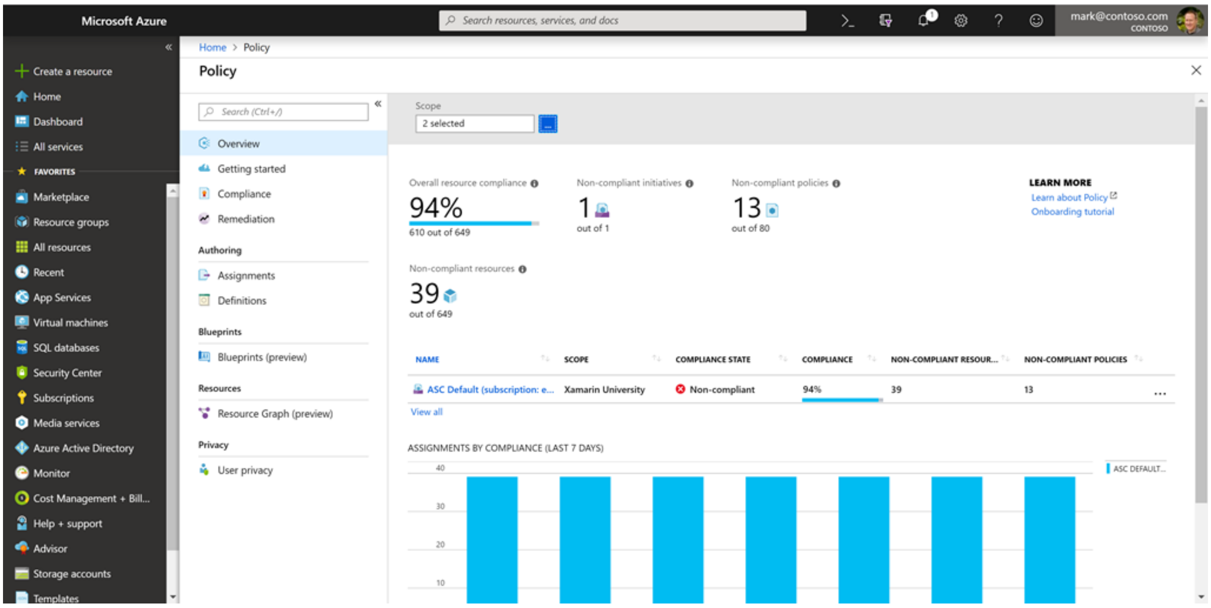
Requests to create or update a resource through Azure Resource Manager are evaluated by Azure Policy first. Policy creates a list of all assignments that apply to the resource and then evaluates the resource against each definition. Policy processes several of the effects before handing the request to the appropriate Resource Provider to avoid any unnecessary processing if the resource violates policy.

Each policy definition in Azure Policy has a single effect. That effect determines what happens when the associated policy rule is matched. When that happens, Azure Policy will take a specific action based on the assigned effect.

Policy Effect	**What happens?**
Deny	The resource creation/update fails due to policy.
Disabled	The policy rule is ignored (disabled). Often used for testing.
Append	Adds additional parameters/fields to the requested resource during creation or update. A common example is adding tags on resources such as Cost Center or specifying allowed IPs for a storage resource.
Audit, AuditIfNotExists	Creates a warning event in the activity log when evaluating a non-compliant resource, but it doesn't stop the request.
DeployIfNotExists	Executes a template deployment when a specific condition is met. For example, if SQL encryption is enabled on a database, then it can run a template after the DB is created to set it up a specific way.

View policy evaluation results

Azure Policy can allow a resource to be created even if it doesn't pass validation. In these cases, you can have it trigger an audit event which can be viewed in the Azure Policy portal, or through command-line tools. The easiest approach is in the portal as it provides a nice graphical overview which you can explore. You can find the Azure Policy section through the search field or *All Services*.



Scope: 2 selected

Overall resource compliance 94% 610 out of 649

Non-compliant initiatives 1 out of 1

Non-compliant policies 13 out of 80

Non-compliant resources 39 out of 649

NAME	SCOPE	COMPLIANCE STATE	COMPLIANCE	NON-COMPLIANT RESOUR...	NON-COMPLIANT POLICIES
ASC Default (subscription: e...	Xamarin University	Non-compliant	94%	39	13

From this screen, you can spot resources which are not compliant and take action to correct them.

Tip

If you continue in the Azure Fundamentals learning path, you'll see Azure Policy in more detail in the Control and organize Azure resources with Azure Resource Manager module.

Organize policy with initiatives

Managing a few policy definitions is easy, but once you have more than a few, you will want to organize them. That's where *initiatives* come in.

Initiatives work alongside policies in Azure Policy. An *initiative definition* is a set or group of policy definitions to help track your compliance state for a larger goal. Even if you have a single policy, we recommend using initiatives if you anticipate increasing the number of policies over time.

Like a policy assignment, an *initiative assignment* is an initiative definition assigned to a specific scope. Initiative assignments reduce the need to make several initiative definitions for each scope. This scope could also range from a management group to a resource group.

Once defined, initiatives can be assigned just as policies can - and they apply all the associated policy definitions.

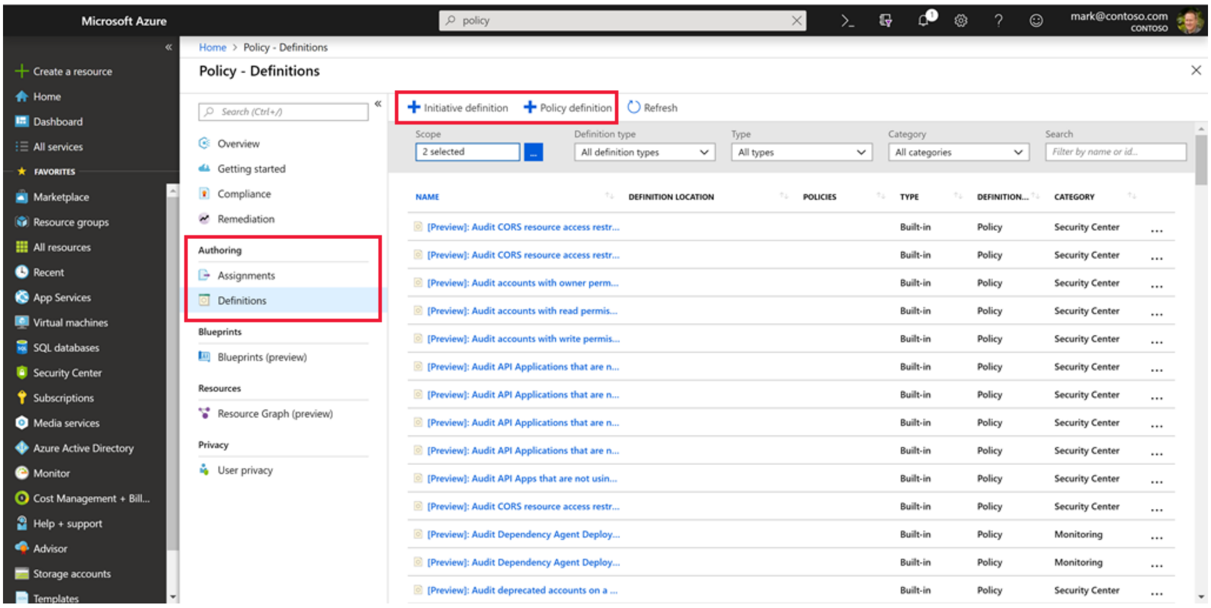
Defining initiatives

Initiative definitions simplify the process of managing and assigning policy definitions by grouping a set of policies into a single item. For example, you could create an initiative named *Enable Monitoring in Azure Security Center*, with a goal to monitor all the available security recommendations in your Azure Security Center.

Under this initiative, you would have the following policy definitions:

Policy definition	Purpose
Monitor unencrypted SQL Database in Security Center	For monitoring unencrypted SQL databases and servers.
Monitor OS vulnerabilities in Security Center	For monitoring servers that do not satisfy the configured baseline.
Monitor missing Endpoint Protection in Security Center	For monitoring servers without an installed endpoint protection agent.

You can define initiatives using the Azure portal, or command-line tools. In the portal, you use the "Authoring" section.



Scope: 2 selected
Definition type: All definition types
Type: All types
Category: All categories
Search: Filter by name or id...

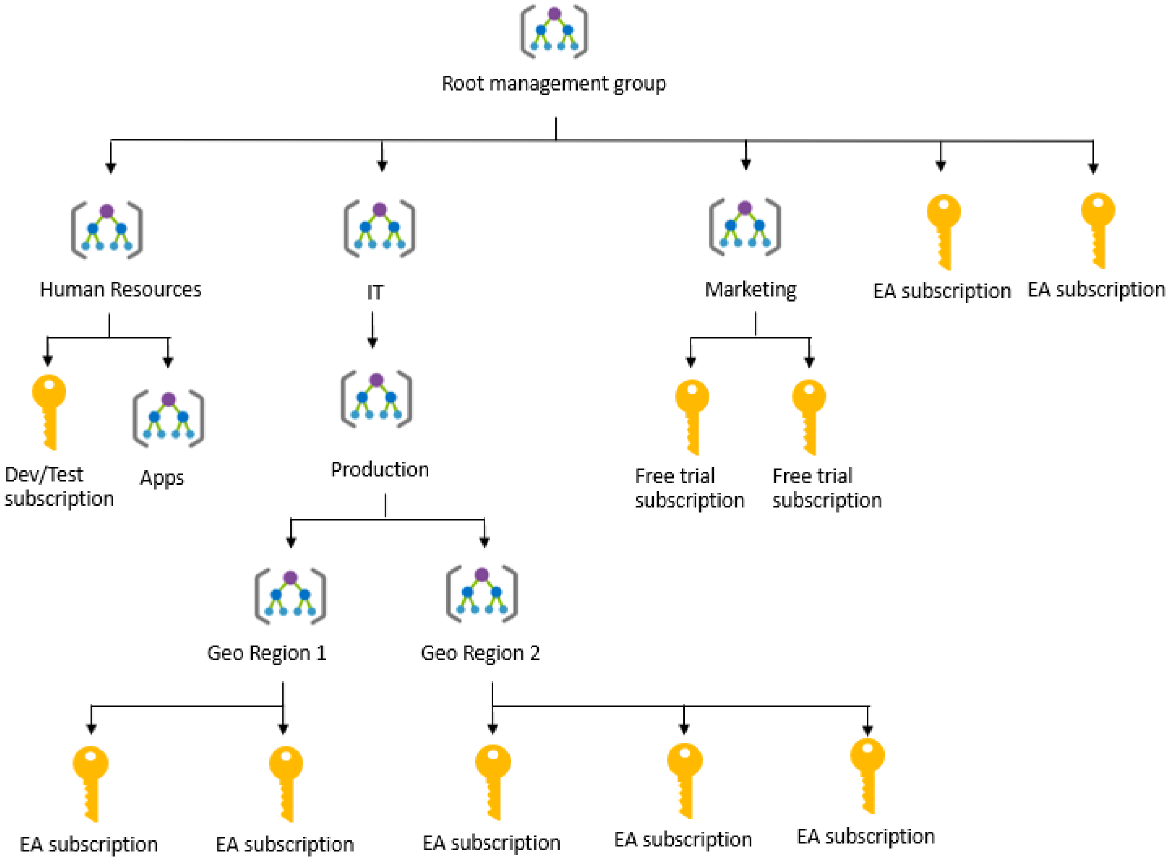
NAME	DEFINITION LOCATION	POLICIES	TYPE	DEFINITION...	CATEGORY	
[Preview]: Audit CORS resource access restr...			Built-in	Policy	Security Center	...
[Preview]: Audit CORS resource access restr...			Built-in	Policy	Security Center	...
[Preview]: Audit accounts with owner perm...			Built-in	Policy	Security Center	...
[Preview]: Audit accounts with read permis...			Built-in	Policy	Security Center	...
[Preview]: Audit accounts with write permis...			Built-in	Policy	Security Center	...
[Preview]: Audit API Applications that are n...			Built-in	Policy	Security Center	...
[Preview]: Audit API Applications that are n...			Built-in	Policy	Security Center	...
[Preview]: Audit API Applications that are n...			Built-in	Policy	Security Center	...
[Preview]: Audit API Applications that are n...			Built-in	Policy	Security Center	...
[Preview]: Audit API Apps that are not usin...			Built-in	Policy	Security Center	...
[Preview]: Audit CORS resource access restr...			Built-in	Policy	Security Center	...
[Preview]: Audit Dependency Agent Deploy...			Built-in	Policy	Monitoring	...
[Preview]: Audit Dependency Agent Deploy...			Built-in	Policy	Monitoring	...
[Preview]: Audit deprecated accounts on a ...			Built-in	Policy	Security Center	...

Enterprise governance management

Access management occurs at the Azure subscription level. This allows an organization to configure each division of the company in a specific fashion based on their responsibilities and requirements. Planning and keeping rules consistent across subscriptions can be challenging without a little help.

Azure Management Groups are containers for managing access, policies, and compliance across *multiple* Azure subscriptions. Management groups allow you to order your Azure resources hierarchically into collections, which provide a further level of classification that is above the level of subscriptions. All subscriptions within a management group automatically inherit the conditions applied to the management group. Management groups give you enterprise-grade management at a large scale no matter what type of subscriptions you might have.

The following diagram shows an example of creating a hierarchy for governance using management groups.



Create a hierarchy so you can apply a policy, for example, limit VM locations to US West Region on the group "Infrastructure Team management group". This policy will inherit onto both EA subscriptions under that management group and will apply to all VMs under those subscriptions. This security policy cannot be altered by the resource or subscription owner allowing for improved governance.

Another scenario where you would use management groups is to provide user access to multi subscriptions. By moving many subscriptions under that management group, you can create one role-based access control (RBAC) assignment on the management group, which will inherit that access to all the subscriptions. One assignment on the management group can enable users to have access to everything they need instead of scripting RBAC rules over different subscriptions.

You can manage your Azure subscriptions more effectively by using Azure Policy and Azure role-based access controls (RBACs). These provide distinct governance conditions that you can apply to each management group. The resources and subscriptions you assign to a management group automatically inherit the conditions that you apply to that management group.

Tip

If you continue in the Azure Fundamentals learning path, you'll learn more about RBAC in the Control and organize Azure resources with Azure Resource Manager module.

Define standard resources with Azure Blueprints

Adhering to security or compliance requirements, whether government or industry requirements, can be difficult and time-consuming. To help you with auditing, traceability, and compliance with your deployments, use **Azure Blueprint** artifacts and tools.

Azure Blueprint allows you to define a repeatable set of Azure resources that implement and adhere to your organization's standards, patterns, and requirements. Blueprint enables development teams to rapidly build and deploy new environments with the knowledge that they're building within organizational compliance with a set of built-in components that speed up development and delivery.

Azure Blueprint is a declarative way to orchestrate the deployment of various resource templates and other artifacts, such as:

- Role assignments
- Policy assignments
- Azure Resource Manager templates
- Resource groups

The process of implementing Azure Blueprint consists of the following high-level steps:

1. Create an Azure Blueprint
2. Assign the blueprint
3. Track the blueprint assignments

With Azure Blueprint, the relationship between the blueprint definition (what *should be* deployed) and the blueprint assignment (what *was* deployed) is preserved. This connection supports improved deployment tracking and auditing.

Azure Blueprints are different from Azure Resource Manager Templates. When Azure Resource Manager Templates deploy resources, they have no active relationship with the deployed resources (they exist in a local environment or source control). By contrast, with Azure Blueprint, each deployment is tied to an Azure Blueprint package. This means that the relationship with resources will be maintained, even after deployment. Managing relationships, in this way, improves auditing and tracking capabilities.

Azure Blueprints are also useful in Azure DevOps scenarios, where blueprints are associated with specific build artifacts and release pipelines and can be tracked more rigorously.

Explore your service compliance with Compliance Manager

Governing your own resources and how they are used is only part of the solution when using a cloud provider. You also have to understand how the *provider* manages the underlying resources you are building on.

Microsoft takes this management very seriously and provides full transparency with four sources:

1. Microsoft Privacy Statement
2. Microsoft Trust Center
3. Service Trust Portal
4. Compliance Manager

Microsoft Privacy Statement

The Microsoft privacy statement explains what personal data Microsoft processes, how Microsoft processes it, and for what purposes.

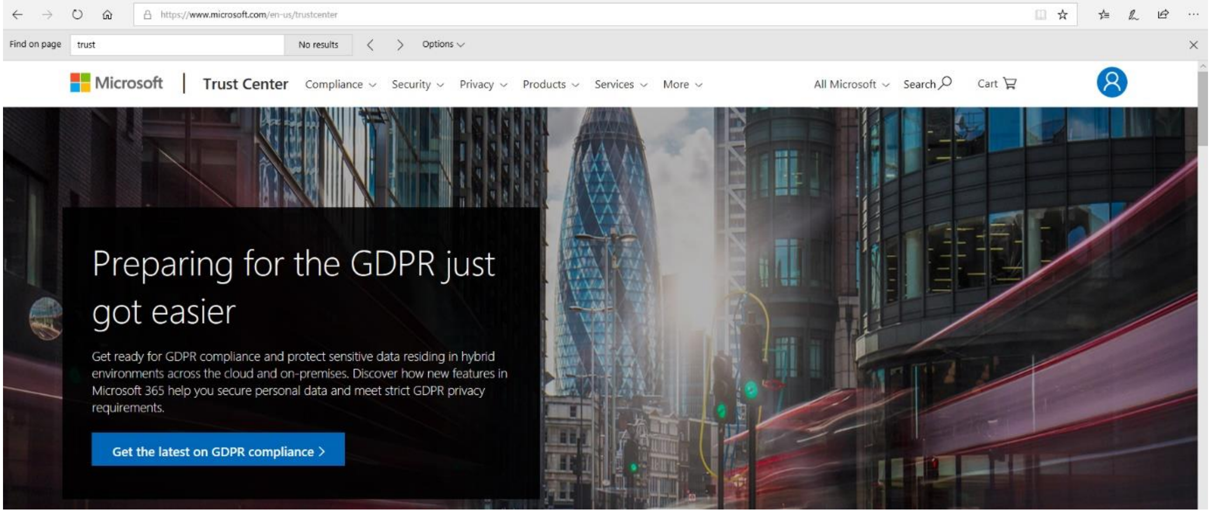
The statement applies to the interactions Microsoft has with you and Microsoft products such as Microsoft services, websites, apps, software, servers, and devices. It is intended to provide openness and honesty about how Microsoft deals with personal data in its products and services.

There is a link to the privacy statement in the summary of this module.

What is the Microsoft Trust Center?

Trust Center is a website resource containing information and details about how Microsoft implements and supports security, privacy, compliance, and transparency in all Microsoft cloud products and services. The Trust Center is an important part of the Microsoft Trusted Cloud Initiative, and provides support and resources for the legal and compliance community including:

- In-depth information about security, privacy, compliance offerings, policies, features, and practices across Microsoft cloud products.
- Recommended resources in the form of a curated list of the most applicable and widely-used resources for each topic.
- Information specific to key organizational roles, including business managers, tenant admins or data security teams, risk assessment and privacy officers, and legal compliance teams.
- Cross-company document search, which is coming soon and will enable existing cloud service customers to search the Service Trust Portal.
- Direct guidance and support for when you can't find what you're looking for.



Preparing for the GDPR just got easier

Get ready for GDPR compliance and protect sensitive data residing in hybrid environments across the cloud and on-premises. Discover how new features in Microsoft 365 help you secure personal data and meet strict GDPR privacy requirements.

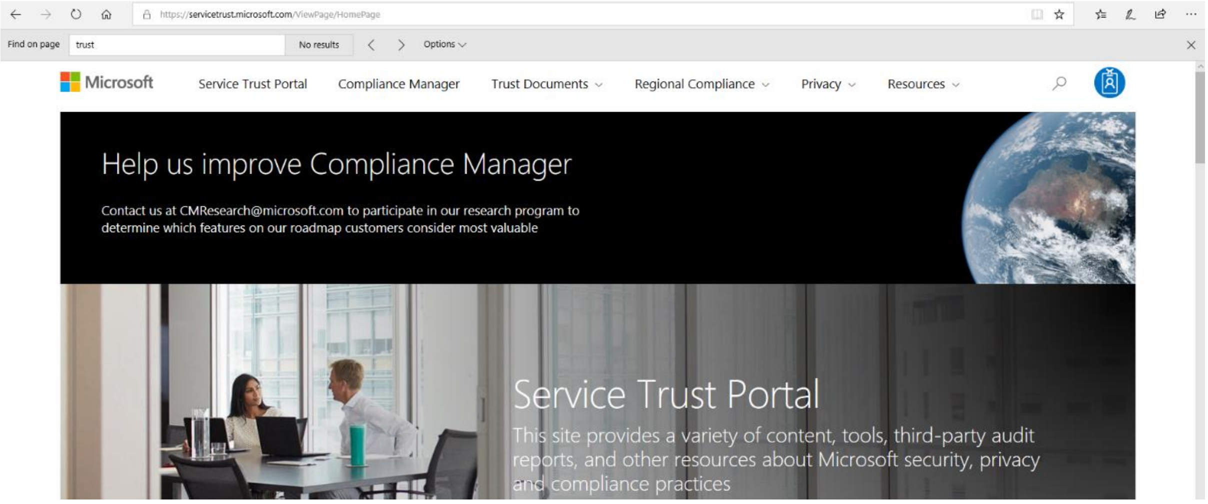
What is the Service Trust Portal?

The **Service Trust Portal** (STP) hosts the Compliance Manager service, and is the Microsoft public site for publishing audit reports and other compliance-related information relevant to Microsoft’s cloud services. STP users can download audit reports produced by external auditors and gain insight from Microsoft-authored reports that provide details on how Microsoft builds and operates its cloud services.

STP also includes information about how Microsoft online services can help your organization maintain and track compliance with standards, laws, and regulations, such as:

- ISO
- SOC
- NIST

- FedRAMP
- GDPR



Help us improve Compliance Manager

Contact us at CMResearch@microsoft.com to participate in our research program to determine which features on our roadmap customers consider most valuable

Service Trust Portal

This site provides a variety of content, tools, third-party audit reports, and other resources about Microsoft security, privacy and compliance practices

Service Trust Portal is a companion feature to the Trust Center, and allows you to:

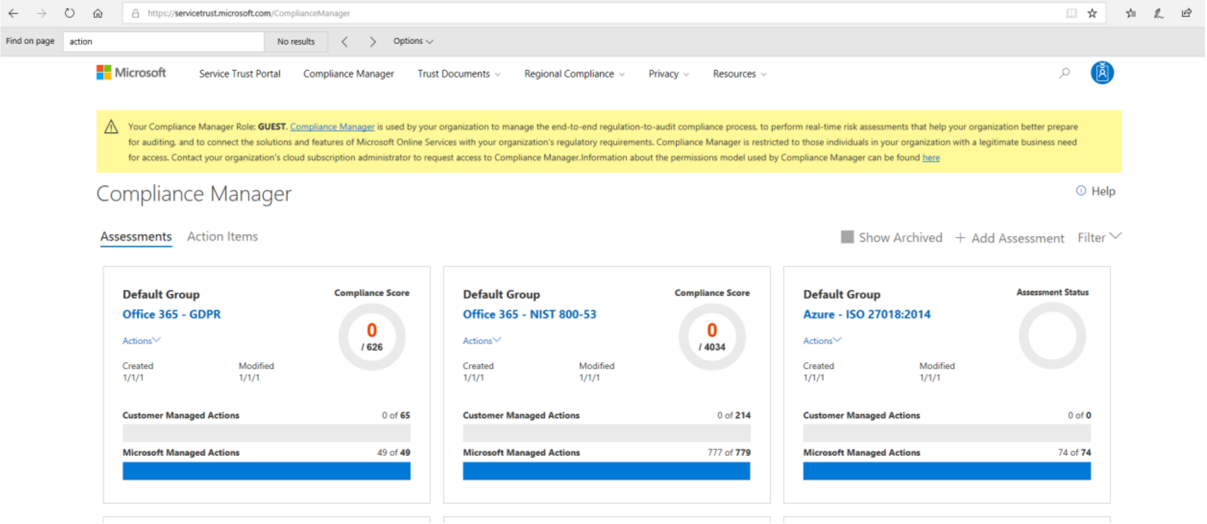
- Access audit reports across Microsoft cloud services on a single page.
- Access compliance guides to help you understand how can you use Microsoft cloud service features to manage compliance with various regulations.
- Access trust documents to help you understand how Microsoft cloud services help protect your data.

Compliance Manager

Compliance Manager is a workflow-based risk assessment dashboard within the Trust Portal that enables you to track, assign, and verify your organization's regulatory compliance activities related to Microsoft professional services and Microsoft cloud services such as Office 365, Dynamics 365, and Azure.

Compliance Manager provides the following features:

- Combines the following three items:
    1. Detailed information provided by Microsoft to auditors and regulators, as part of various third-party audits of Microsoft 's cloud services against various standards (for example, ISO 27001, ISO 27018, and NIST).
    2. Information that Microsoft compiles internally for its compliance with regulations (such as HIPAA and the EU GDPR).
    3. An organization's self-assessment of their own compliance with these standards and regulations.
- Enables you to assign, track, and record compliance and assessment-related activities, which can help your organization cross team barriers to achieve your organization's compliance goals.
- Provides a Compliance Score to help you track your progress and prioritize auditing controls that will help reduce your organization's exposure to risk.
- Provides a secure repository in which to upload and manage evidence and other artifacts related to compliance activities.
- Produces richly detailed reports in Microsoft Excel that document the compliance activities performed by Microsoft and your organization, which can be provided to auditors, regulators, and other compliance stakeholders.



Your Compliance Manager Role: **GUEST**. Compliance Manager is used by your organization to manage the end-to-end regulation-to-audit compliance process, to perform real-time risk assessments that help your organization better prepare for auditing, and to connect the solutions and features of Microsoft Online Services with your organization's regulatory requirements. Compliance Manager is restricted to those individuals in your organization with a legitimate business need for access. Contact your organization's cloud subscription administrator to request access to Compliance Manager.Information about the permissions model used by Compliance Manager can be found here

Compliance Manager

Default Group
Office 365 - GDPR
Compliance Score 0 / 626
Created 1/1/1 Modified 1/1/1
Customer Managed Actions 0 of 65
Microsoft Managed Actions 49 of 49

Default Group
Office 365 - NIST 800-53
Compliance Score 0 / 4034
Created 1/1/1 Modified 1/1/1
Customer Managed Actions 0 of 214
Microsoft Managed Actions 777 of 779

Default Group
Azure - ISO 27018:2014
Assessment Status
Created 1/1/1 Modified 1/1/1
Customer Managed Actions 0 of 0
Microsoft Managed Actions 74 of 74

Compliance Manager provides ongoing risk assessments with a risk-based scores reference displayed in a dashboard view for regulations and standards. Alternatively, you can create assessments for the regulations or standards that matter more to your organization.

As part of the risk assessment, Compliance Manager also provides recommended actions you can take to improve your regulatory compliance. You can view all action items, or select the action items that correspond with a specific certification.

Important

Compliance Manager is a dashboard that provides a summary of your data protection and compliance stature and recommendations for improvement. The Customer Actions provided in Compliance Manager are recommendations only; it is up to each organization to evaluate the effectiveness of these recommendations in their respective regulatory environment prior to implementation. Recommendations found in Compliance Manager should not be interpreted as a guarantee of compliance.

Monitor your service health

Defining policy and access provides fine-grained control over resources in your cloud IT infrastructure. Once those resources are deployed, you will want to know about any issues or performance problems they might encounter.

Azure provides two primary services to monitor the health of your apps and resources.

1. Azure Monitor
2. Azure Service Health

Azure Monitor

Azure Monitor maximizes the availability and performance of your applications by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. It helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.

Data sources

Azure Monitor can collect data from a variety of sources. You can think of monitoring data for your applications in tiers ranging from your application, any operating system and services it relies on, down to the platform itself.

Data tier	Description
Application monitoring data	Data about the performance and functionality of the code you have written, regardless of its platform.
Guest OS monitoring data	Data about the operating system on which your application is running. This could be running in Azure, another cloud, or on-premises.
Azure resource monitoring data	Data about the operation of an Azure resource.
Azure subscription monitoring data	Data about the operation and management of an Azure subscription, as well as data about the health and operation of Azure itself.
Azure tenant monitoring data	Data about the operation of tenant-level Azure services, such as Azure Active Directory.

Diagnostic settings

As soon as you create an Azure subscription and start adding resources such as virtual machines and web apps, Azure Monitor starts collecting data. *Activity Logs* record when resources are created or modified and *Metrics* tell you how the resource is performing and the resources that it's consuming.

You can extend the data you're collecting into the actual operation of the resources by enabling **diagnostics** and adding an agent to compute resources. Under the resource settings you can enable Diagnostics

- *Enable guest-level monitoring*
- *Performance counters*: collect performance data
- *Event Logs*: enable various event logs
- *Crash Dumps*: enable or disable
- *Sinks*: send your diagnostic data to other services for more analysis
- *Agent*: configure agent settings

Getting more data from your apps

Data monitoring is only useful if it improves your visibility of the operations in your computing environment. Azure Monitor includes several features and tools that provide valuable insights into your applications, and the other resources they may depend on.

Application Insights is a service that monitors the availability, performance, and usage of your web applications, whether they're hosted in the cloud or on-premises.

It leverages the powerful data analysis platform in Log Analytics to provide you with deeper insights into your application's operations. Application Insights can diagnose errors, without waiting for a user to report them. Application Insights includes connection points to a variety of development tools, and integrates with Microsoft Visual Studio to support your DevOps processes.

Azure Monitor for containers is a service that is designed to monitor the performance of container workloads, which are deployed to managed Kubernetes clusters hosted on Azure Kubernetes Service (AKS). It gives you performance visibility by collecting memory and processor metrics from controllers, nodes, and containers, which are available in Kubernetes through the metrics API. Container logs are also collected.

Azure Monitor for VMs is a service that monitors your Azure VMs at scale, by analyzing the performance and health of your Windows and Linux VMs (including their different processes and interconnected dependencies on other resources, and external processes). Azure Monitor for VMs includes support for monitoring performance and application dependencies for VMs hosted on-premises, and for VMs hosted with other cloud providers.

Integrating any, or all, of these monitoring services with Azure Service Health has additional benefits. Staying informed of the health status of Azure services will help you understand if, and when, an issue affecting an Azure service is impacting your environment. What may seem like a localized problem could be the result of a more widespread issue, and Azure Service Health provides this kind of insight. Azure Service Health identifies any issues with Azure services that might affect your application. Azure Service Health also helps you to plan for scheduled maintenance.

Responding to alert conditions

In addition to allowing you to analyze your monitoring data interactively, an effective monitoring solution must respond proactively to any critical conditions that are identified within the data it collects. This might involve, for example, sending a text or email to an administrator who is responsible for investigating an issue, or launching an automated process that attempts to correct an error condition.

Alerts. Azure Monitor proactively notifies you of critical conditions using alerts, and can potentially attempt to take corrective actions. Alert rules based on metrics can provide alerts in almost real-time, based on numeric values. Alert rules based on logs allow for complex logic across data, from multiple sources.

Autoscale. Azure Monitor uses Autoscale to ensure that you have the right amount of resources running to manage the load on your application effectively. Autoscale enables you to create rules that use metrics, collected by Azure Monitor, to determine when to automatically add resources to handle increases in load. Autoscale can also help reduce your Azure costs by removing resources that are not being used. You can specify a minimum and maximum number of instances, and provide the logic that determines when Autoscale should increase or decrease resources.

Visualize monitoring data

Visualizations, such as charts and tables, are effective tools for summarizing monitoring data and for presenting data to different audiences. Azure Monitor has its own features for visualizing monitoring data, and it leverages other Azure services for publishing data for different audiences. Other tools you may use for visualizing data, for particular audiences and scenarios, include:

- Dashboards
- Views
- Power BI

Integrate with other services

You'll often need to integrate Azure Monitor with other systems, and build customized solutions that use your monitoring data. Other Azure services can work with Azure Monitor to provide this integration.

Azure Service Health

Azure Service Health is a suite of experiences that provide personalized guidance and support when issues with Azure services affect you. It can notify you, help you understand the impact of issues, and keep you updated as the issue is resolved. Azure Service Health can also help you prepare for planned maintenance and changes that could affect the availability of your resources.

Azure Service Health is composed of the following views.

Azure Status provides a global view of the health state of Azure services. With Azure Status, you can get up-to-the-minute information on service availability. Everyone has access to Azure Status and can view all services that report their health state.

Service Health provides you with a customizable dashboard that tracks the state of your Azure services in the regions where you use them. In this dashboard, you can track active events such as ongoing service issues, upcoming planned maintenance, or relevant *Health advisories*. When events become inactive, they are placed in your *Health history* for up to 90 days. Finally, you can use the **Service Health** dashboard to create and manage service *Health alerts*, which notify you whenever there are service issues that affect you.

Resource Health helps you diagnose and obtain support when an Azure service issue affects your resources. It provides you with details about the current and past state of your resources. It also provides technical support to help you mitigate problems. In contrast to Azure Status, which informs you about service problems that affect a broad set of Azure customers, *Resource Health* gives you a personalized dashboard of your resources' health. *Resource Health* shows you times, in the past, when your resources were unavailable because of Azure service problems. It's then easier for you to understand if an SLA was violated.

Together, the Azure Service Health components provide you with a comprehensive view of the health status of Azure, at the level of granularity that is most relevant to you.

Summary

In this module you've learned about Azure governance methodologies, monitoring and reporting in Azure, and privacy, compliance, and data protection standards in Azure.

Learn More

Here are some places to go to learn more about what we've covered today:

- Microsoft Privacy Statement
- Microsoft Trust Center
- Service Trust Portal
- Azure Service Health
- Azure Monitor
- Azure Status