Introduction

In this module, you'll be introduced to some of the features and tools you can use to help with governance of your Azure environment. You'll also learn about tools you can use to help keep resources in compliance with corporate or regulatory requirements.

Learning objectives

After completing this module, you'll be able to:

- Describe the purpose of Microsoft Purview.
- Describe the purpose of Azure Policy.
- Describe the purpose of resource locks.
- Describe the purpose of the Service Trust portal.

Describe the purpose of Microsoft Purview

Microsoft Purview is a family of data governance, risk, and compliance solutions that helps you get a single, unified view into your data. Microsoft Purview brings insights about your on-premises, multicloud, and software-as-a-service data together.

With Microsoft Purview, you can stay up-to-date on your data landscape thanks to:

- Automated data discovery
- Sensitive data classification
- End-to-end data lineage

Two main solution areas comprise Microsoft Purview: **risk and compliance** and **unified data governance**.

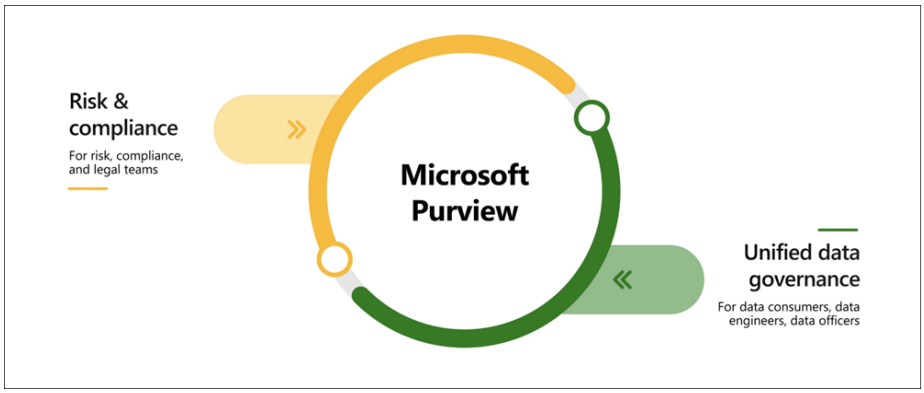

Figure 1: Illustration showing the main areas for Microsoft Purview.

Microsoft Purview risk and compliance solutions

Microsoft 365 features as a core component of the Microsoft Purview risk and compliance solutions. Microsoft Teams, OneDrive, and Exchange are just some of the Microsoft 365 services that Microsoft Purview uses to help manage and monitor your data. Microsoft Purview, by managing and monitoring your data, is able to help your organization:

- Protect sensitive data across clouds, apps, and devices.
- Identify data risks and manage regulatory compliance requirements.
- Get started with regulatory compliance.

Unified data governance

Microsoft Purview has robust, unified data governance solutions that help manage your on-premises, multicloud, and software as a service data. Microsoft Purview's robust data governance capabilities enable you to manage your data stored in Azure, SQL and Hive databases, locally, and even in other clouds like Amazon S3.

Microsoft Purview's unified data governance helps your organization:

- Create an up-to-date map of your entire data estate that includes data classification and end-to-end lineage.
- Identify where sensitive data is stored in your estate.
- Create a secure environment for data consumers to find valuable data.
- Generate insights about how your data is stored and used.
- Manage access to the data in your estate securely and at scale.

Describe the purpose of Azure Policy

How do you ensure that your resources stay compliant? Can you be alerted if a resource's configuration has changed?

Azure Policy is a service in Azure that enables you to create, assign, and manage policies that control or audit your resources. These policies enforce different rules across your resource configurations so that those configurations stay compliant with corporate standards.

How does Azure Policy define policies?

Azure Policy enables you to define both individual policies and groups of related policies, known as initiatives. Azure Policy evaluates your resources and highlights resources that aren't compliant with the policies you've created. Azure Policy can also prevent noncompliant resources from being created.

Azure Policies can be set at each level, enabling you to set policies on a specific resource, resource group, subscription, and so on. Additionally, Azure Policies

are inherited, so if you set a policy at a high level, it will automatically be applied to all of the groupings that fall within the parent. For example, if you set an Azure Policy on a resource group, all resources created within that resource group will automatically receive the same policy.

Azure Policy comes with built-in policy and initiative definitions for Storage, Networking, Compute, Security Center, and Monitoring. For example, if you define a policy that allows only a certain size for the virtual machines (VMs) to be used in your environment, that policy is invoked when you create a new VM and whenever you resize existing VMs. Azure Policy also evaluates and monitors all current VMs in your environment, including VMs that were created before the policy was created.

In some cases, Azure Policy can automatically remediate noncompliant resources and configurations to ensure the integrity of the state of the resources. For example, if all resources in a certain resource group should be tagged with AppName tag and a value of "SpecialOrders," Azure Policy will automatically apply that tag if it is missing. However, you still retain full control of your environment. If you have a specific resource that you don't want Azure Policy to automatically fix, you can flag that resource as an exception – and the policy won't automatically fix that resource.

Azure Policy also integrates with Azure DevOps by applying any continuous integration and delivery pipeline policies that pertain to the pre-deployment and post-deployment phases of your applications.

What are Azure Policy initiatives?

An Azure Policy initiative is a way of grouping related policies together. The initiative definition contains all of the policy definitions to help track your compliance state for a larger goal.

For example, Azure Policy includes an initiative named Enable Monitoring in Azure Security Center. Its goal is to monitor all available security recommendations for all Azure resource types in Azure Security Center.

Under this initiative, the following policy definitions are included:

- **Monitor unencrypted SQL Database in Security Center** This policy monitors for unencrypted SQL databases and servers.
- **Monitor OS vulnerabilities in Security Center** This policy monitors servers that don't satisfy the configured OS vulnerability baseline.
- **Monitor missing Endpoint Protection in Security Center** This policy monitors for servers that don't have an installed endpoint protection agent.

In fact, the Enable Monitoring in Azure Security Center initiative contains over 100 separate policy definitions.

Describe the purpose of resource locks

A resource lock prevents resources from being accidentally deleted or changed.

Even with Azure role-based access control (Azure RBAC) policies in place, there's still a risk that people with the right level of access could delete critical cloud resources. Resource locks prevent resources from being deleted or updated, depending on the type of lock. Resource locks can be applied to individual resources, resource groups, or even an entire subscription. Resource locks are inherited, meaning that if you place a resource lock on a resource group, all of the resources within the resource group will also have the resource lock applied.

Types of Resource Locks

There are two types of resource locks, one that prevents users from deleting and one that prevents users from changing or deleting a resource.

- Delete means authorized users can still read and modify a resource, but they can't delete the resource.
- ReadOnly means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

How do I manage resource locks?

You can manage resource locks from the Azure portal, PowerShell, the Azure CLI, or from an Azure Resource Manager template.

To view, add, or delete locks in the Azure portal, go to the Settings section of any resource's Settings pane in the Azure portal.

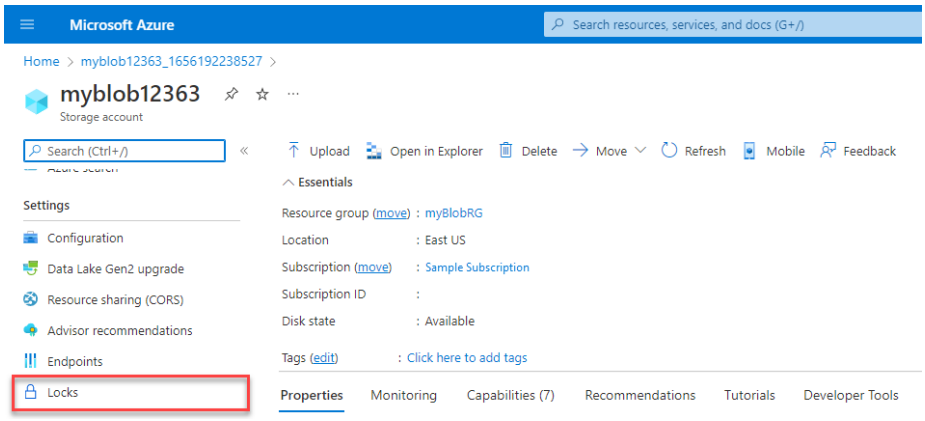

Figure 2: A screenshot showing the resource lock control, under settings, for a storage account.

How do I delete or change a locked resource?

Although locking helps prevent accidental changes, you can still make changes by following a two-step process.

To modify a locked resource, you must first remove the lock. After you remove the lock, you can apply any action you have permissions to perform. Resource locks apply regardless of RBAC permissions. Even if you're an owner of the resource, you must still remove the lock before you can perform the blocked activity.

Describe the purpose of the Service Trust portal

The Microsoft Service Trust Portal is a portal that provides access to various content, tools, and other resources about Microsoft security, privacy, and compliance practices.

The Service Trust Portal contains details about Microsoft's implementation of controls and processes that protect our cloud services and the customer data therein. To access some of the resources on the Service Trust Portal, you must sign in as an authenticated user with your Microsoft cloud services account (Microsoft Entra organization account). You'll need to review and accept the Microsoft non-disclosure agreement for compliance materials.

Accessing the Service Trust Portal

You can access the Service Trust Portal at https://servicetrust.microsoft.com/.

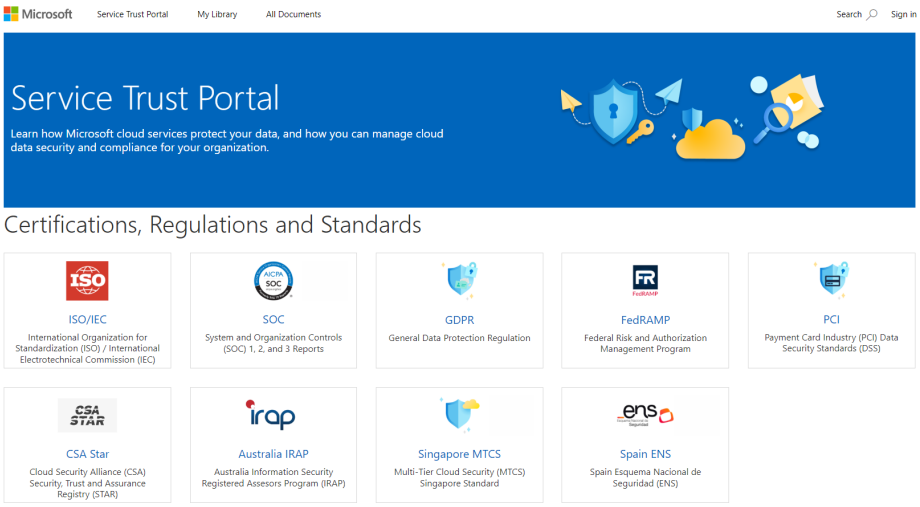

Figure 3: Screenshot of the service trust portal with the main menu items visible.

The Service Trust Portal features and content are accessible from the main menu. The categories on the main menu are:

- **Service Trust Portal** provides a quick access hyperlink to return to the Service Trust Portal home page.
- **My Library** lets you save (or pin) documents to quickly access them on your My Library page. You can also set up to receive notifications when documents in your My Library are updated.

- **All Documents** is a single landing place for documents on the service trust portal. From **All Documents**, you can pin documents to have them show up in your **My Library**.

  [!info] Note Service Trust Portal reports and documents are available to download for at least 12 months after publishing or until a new version of document becomes available.