Microsoft Security

SC-900

Learning Path: 04

Describe the Capabilities of Microsoft Compliance Solutions

M365
Purview

Azure
Policies
Blue Prints

Learning Path Agenda

Describe the Service Trust Portal and privacy with Microsoft.

Describe the compliance management capabilities in Microsoft Purview.

Describe information protection and data lifecycle management capabilities in Microsoft Purview.

Describe insider risk capabilities in Microsoft Purview.

Describe eDiscovery & audit capabilities in Microsoft Purview.

Describe resource governance capabilities in Azure.

Module 1: Describe the Service Trust Portal and privacy with Microsoft

Module 1 Introduction

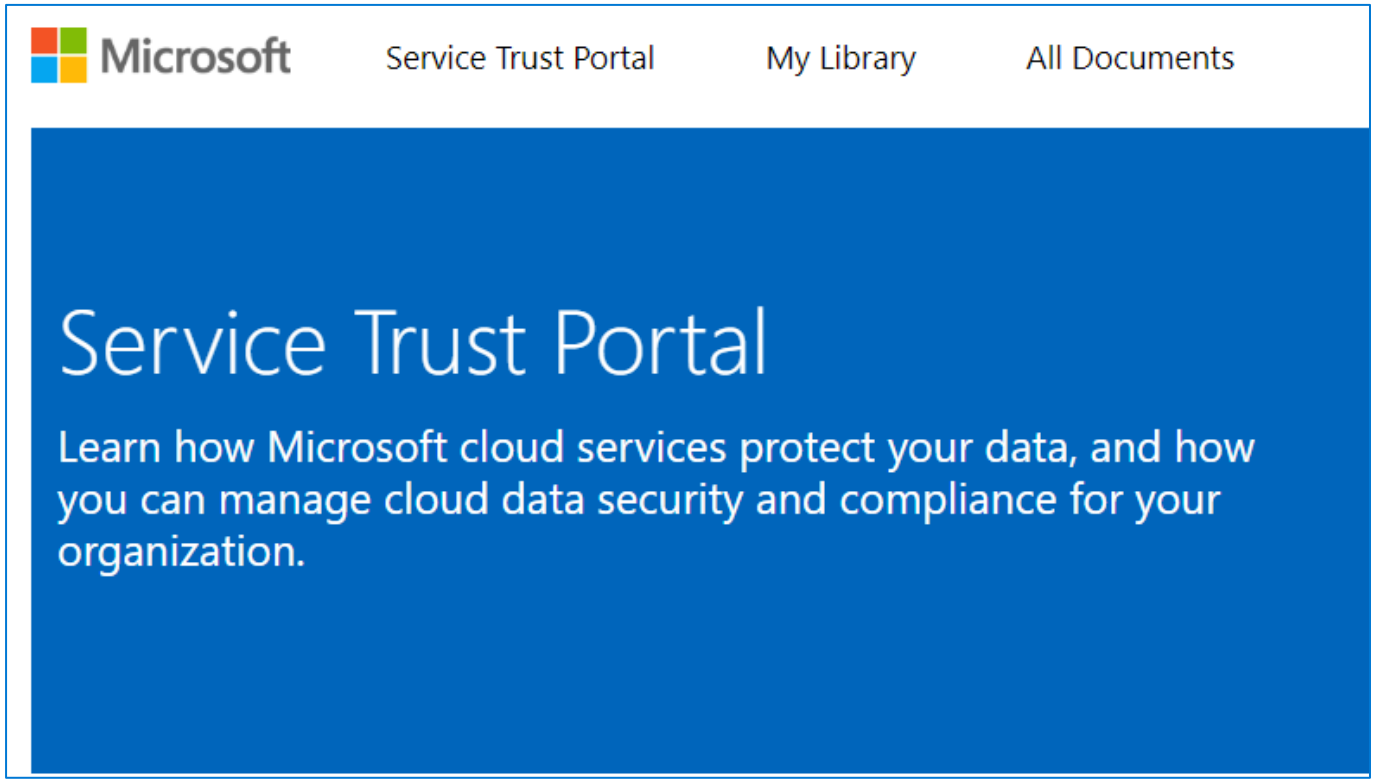
After completing this module, you should be able to:

- Describe the benefit of the Service Trust Portal.
- Describe Microsoft's privacy principles.
- Describe Microsoft Priva.

Microsoft Service Trust Portal

Microsoft's site for publishing audit reports and other compliance-related information associated with Microsoft's cloud services.

- Certifications, Regulations and Standards
- Reports, Whitepapers and Artifacts
- Industry and Regional Resources
- Resources for your Organization



Microsoft Security

Demo

Service Trust Portal

Microsoft's privacy principles

Control: Putting you, the customer, in control of your privacy with easy-to-use tools and clear choices.

Transparency: Being transparent about data collection and use so that everyone can make informed decisions.

Security: Protecting the data that's entrusted to Microsoft by using strong security and encryption.

Strong legal protections: Respecting local privacy laws and fighting for legal protection of privacy as a fundamental human right.

No content-based targeting: Not using email, chat, files, or other personal content to target advertising.

Benefits to you: When Microsoft does collect data, it's used to benefit you, the customer, and to make your experiences better.

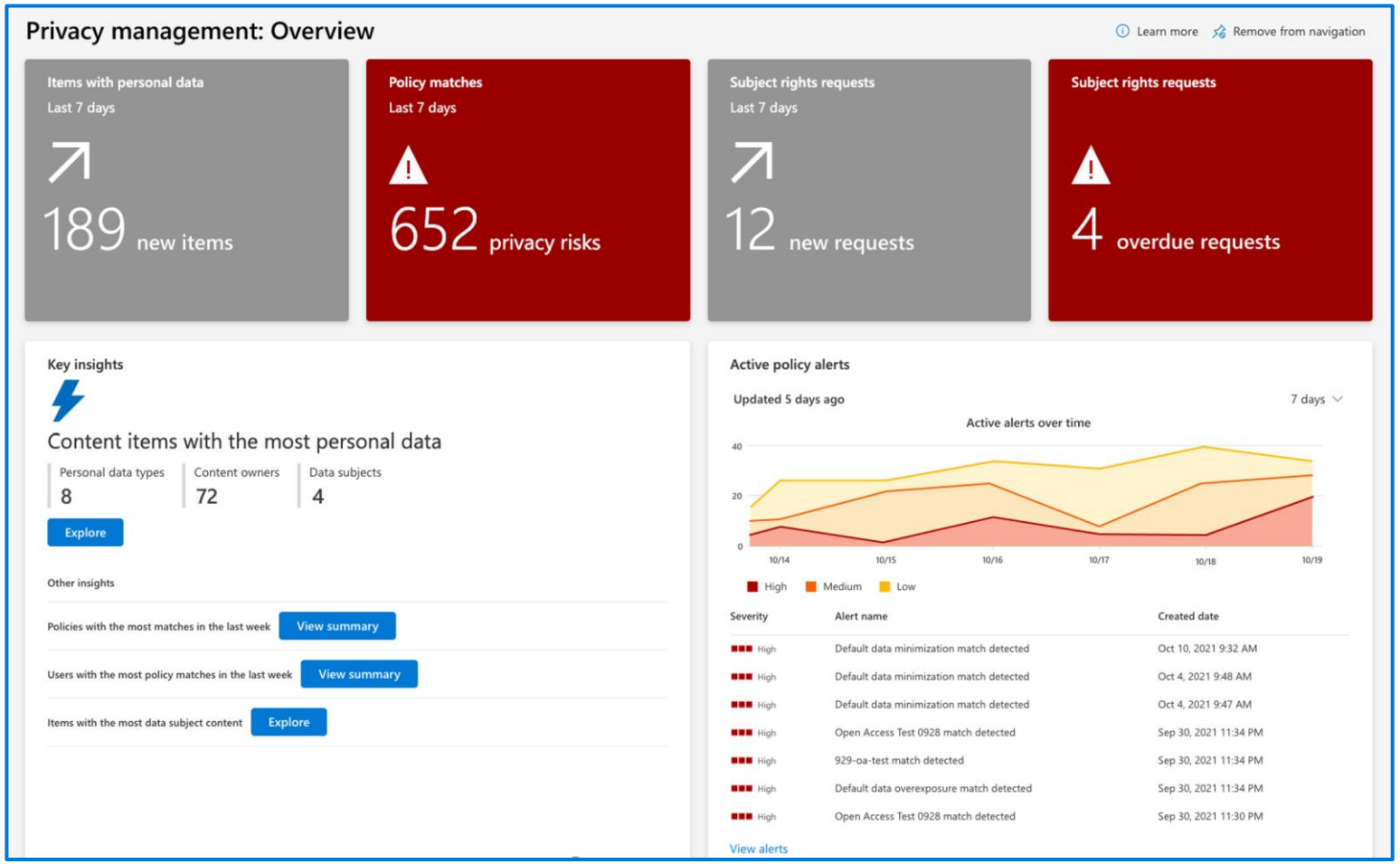
Microsoft Priva

Priva Privacy Risk Management

- Overview dashboard provides automatic updates about your data with important trends.
- Data profile provides a snapshot view of the personal data your organization stores in Microsoft 365 and where it lives.
- Set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation.

Priva Subject Rights Requests

Workflow, automation, and collaboration capabilities to help search for subject data, review findings, collect the appropriate files, and produce reports.



Module 2: Describe the compliance management capabilities in Microsoft Purview

Module 2 Introduction

After completing this module, you should be able to:

- Explore the Microsoft Purview compliance portal.
- Describe Compliance Manager.
- Describe the use and benefits of compliance score.

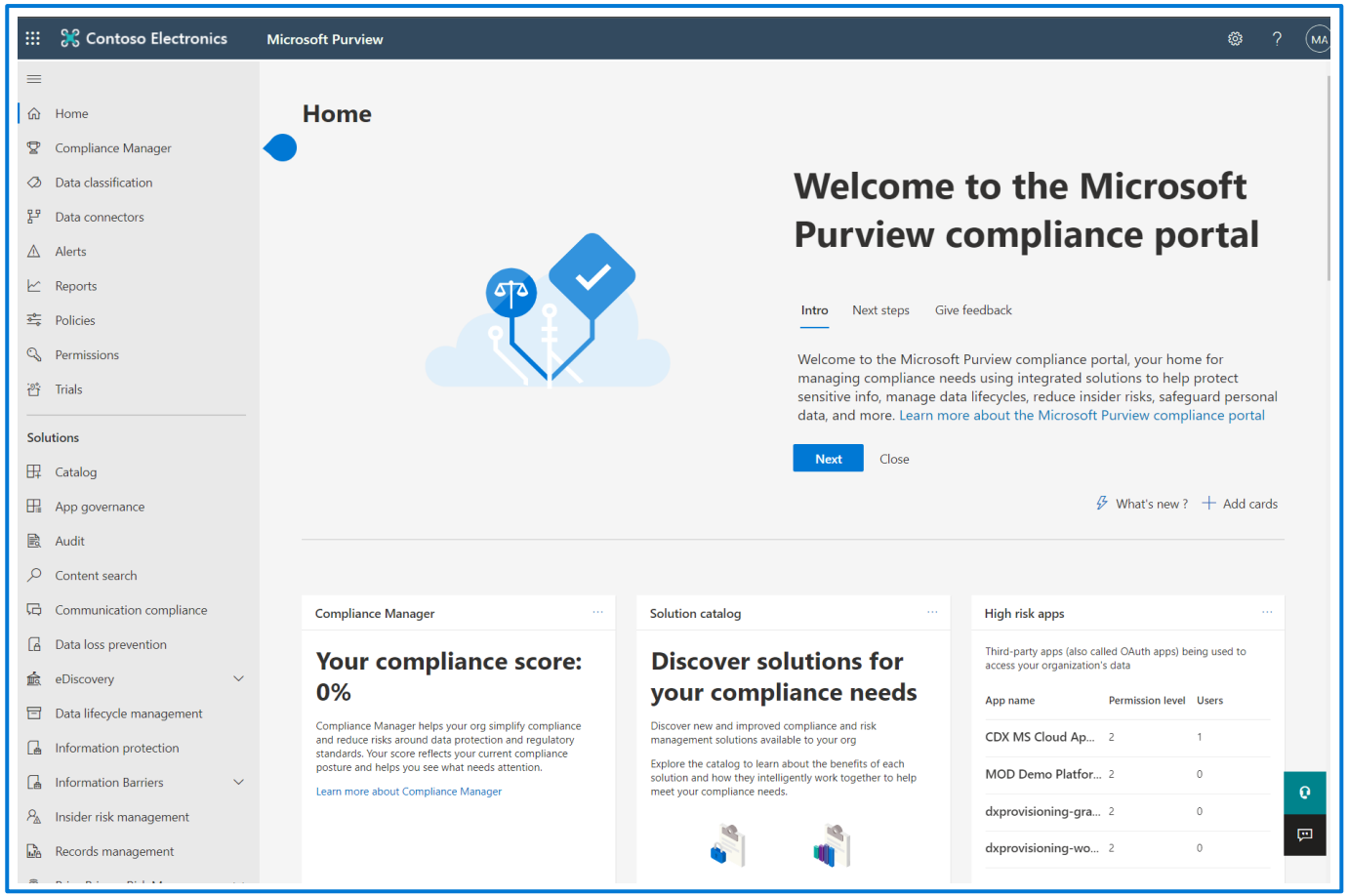
Microsoft Purview compliance portal

Microsoft Purview compliance portal

- A view of how the organization is meeting its compliance requirements.
- Solutions that can be used to help with compliance.
- Information about active alerts.
- And more...

Navigation

- Access to alerts, reports, policies, compliance solutions, and more.
- Add or remove options for a customized navigation pane.
- Customize navigation control.



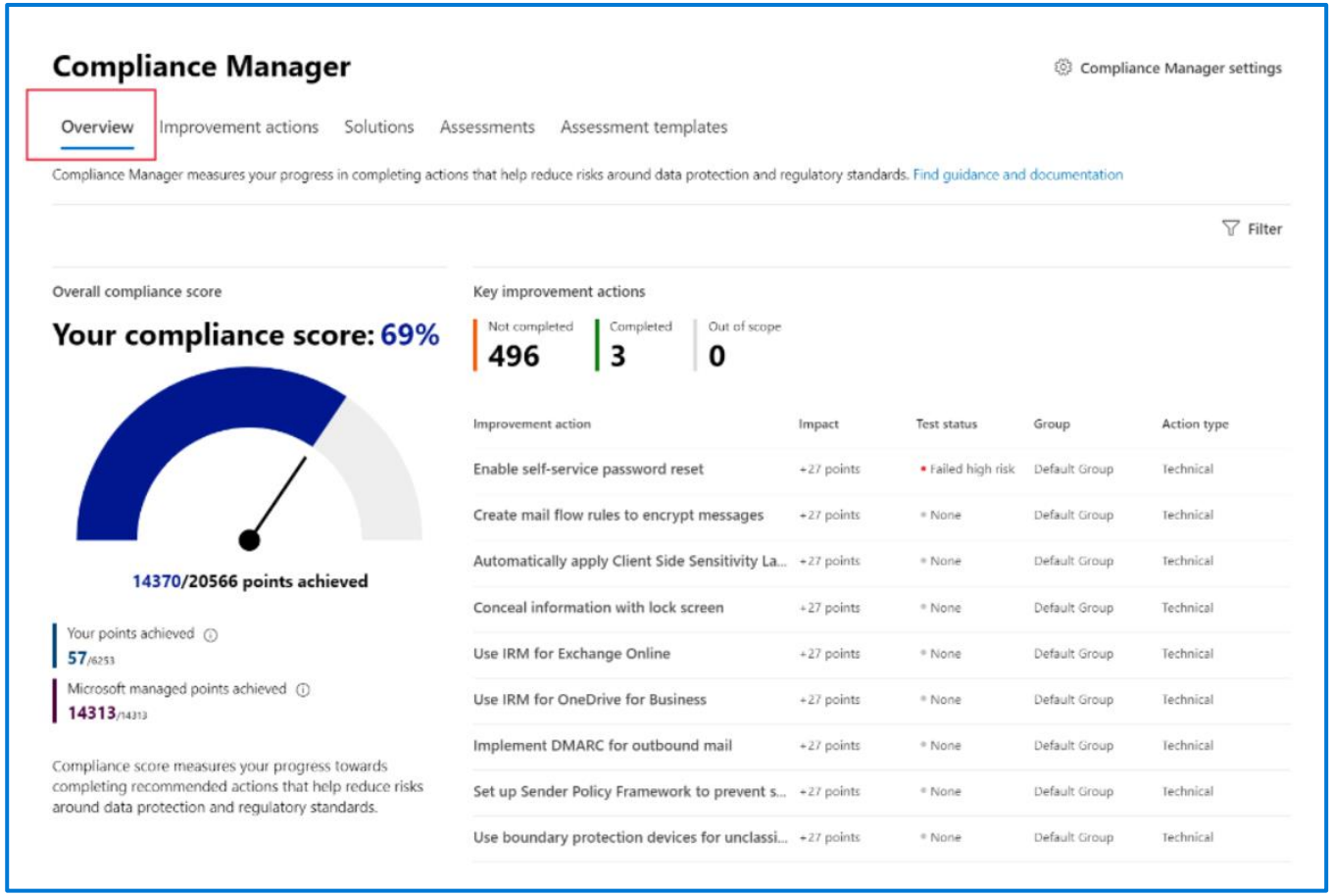
Compliance Manager

Compliance Manager simplifies compliance and reduces risk by providing:

- Prebuilt assessments based on common standards
- Workflow capabilities to complete risk assessments
- Step-by-step improvement actions
- Compliance score, shows overall compliance posture

Key elements of Compliance Manager

- Controls
- Assessments
- Templates
- Improvement actions



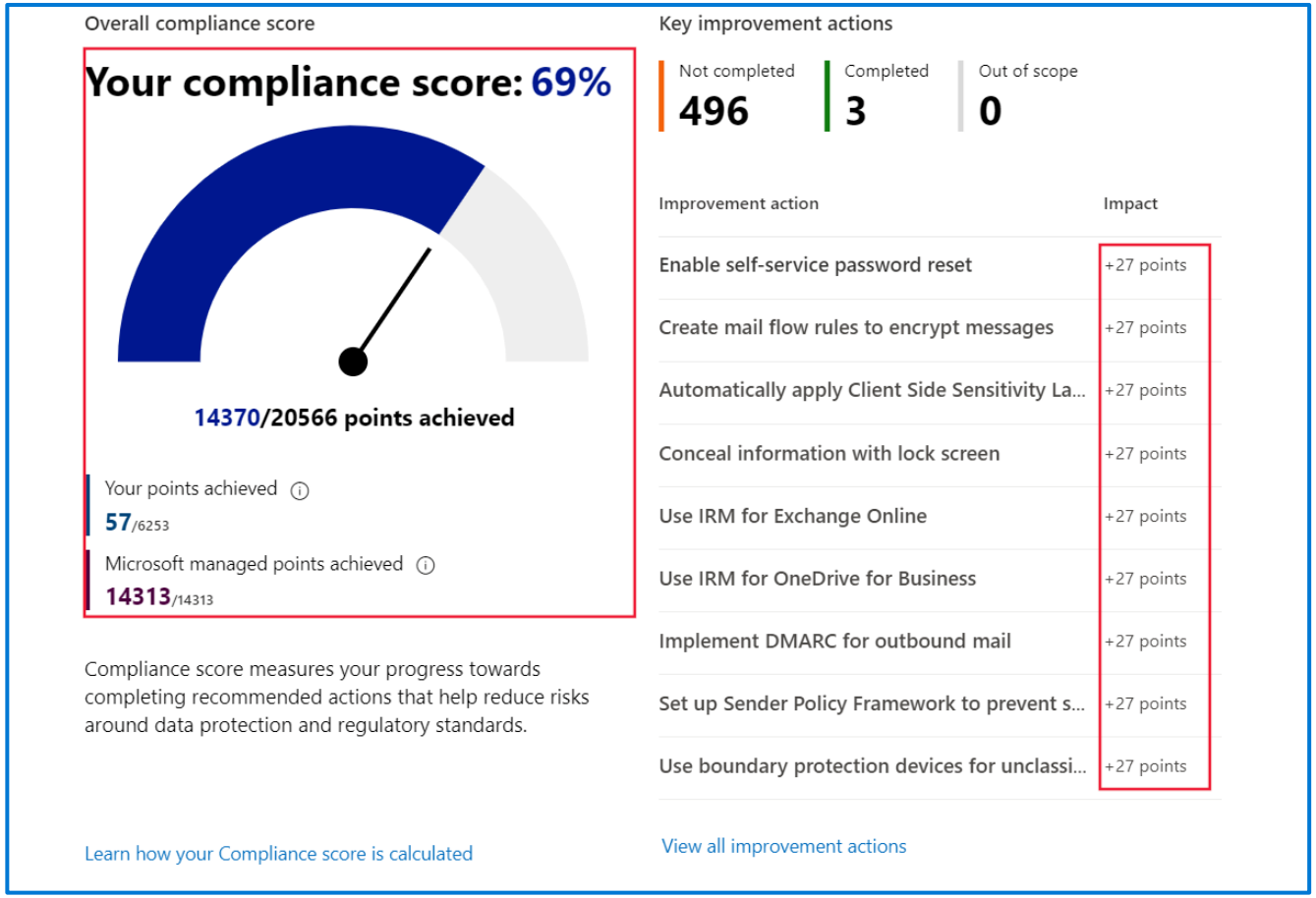
Compliance score

Benefits of compliance score:

- Help an organization understand its current compliance posture.
- Help prioritize actions based on their potential to reduce risk.

Understand your compliance score

- Actions
  - Your improved actions
  - Microsoft actions
- Action types (& action subcategory)
  - Mandatory (preventive, detective, or corrective)
  - Discretionary (preventive, detective, or corrective)



Microsoft Security

Demo

Microsoft Purview compliance portal

Module 3: Describe information protection and data lifecycle management in Microsoft Purview

Module 3 Introduction

After completing this module, you should be able to:

- Describe data classification capabilities.
- Describe records management.
- Describe data loss prevention.

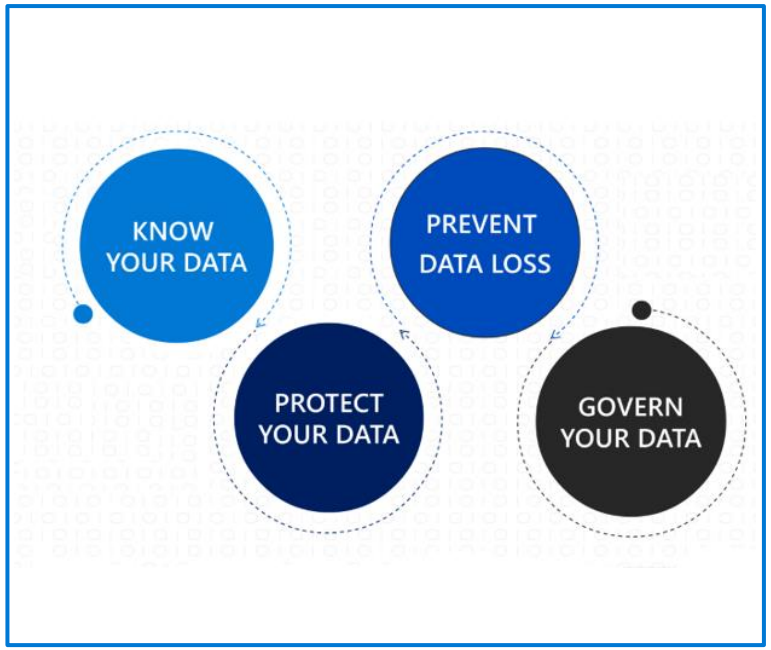
Know your data, protect your data, and govern your data

Know your data: Understand your data landscape and identify important data across on-premises, cloud, and hybrid environments.

Protect your data: Apply flexible protection actions including encryption, access restrictions, and visual markings.

Prevent data loss: Detect risky behavior and prevent accidental oversharing of sensitive information.

Govern your data: Automatically keep, delete, and store data and records in a compliant manner.



Data classification capabilities of the compliance portal

Sensitive information types.

Trainable classifiers: Pre-trained classifiers and Custom trainable classifiers.

Understand and explore the data.

The content explorer: It enables administrators to gain visibility into the content that has been summarized in the overview pane.

The activity explorer: It can monitor what's being done with labeled content across the organization.

Sensitivity labels and policies

Sensitivity labels

Labels are:

- Customizable
- Clear text
- Persistent

Usage:

- Encrypt email and documents.
- Mark the content.
- Apply the label automatically.
- Protect content in containers: sites and groups.
- Extend sensitivity labels to third-party apps and services.
- Classify content without using any protection settings.

Label policies

Policies enable admins to:

- Choose the users and groups that can see labels.
- Apply a default label to all new emails and documents.
- Require justifications for label changes.
- Require users to apply a label (mandatory labeling).
- Link users to custom help pages.

Once a sensitivity label is applied to an email or document, any configured protection settings for that label are enforced on the content.

Microsoft Security

Demo

Sensitivity labels

Data loss prevention (DLP)

DLP protects sensitive information and prevents its inadvertent disclosure.

- DLP policies protect information by identifying and automatically protecting sensitive data.
- Protect sensitive information across Microsoft 365 – OneDrive for Business, SharePoint Online, Exchange Online and Microsoft Teams.

Endpoint Data Loss Prevention

- DLP extended to Windows 10 devices.
- Audit and manage activities including creating, coping, printing, & renaming items.

Data Loss Prevention in Microsoft Teams

- DLP capabilities extended to Microsoft Teams chat and channel message.

Retention labels and policies

Retention settings work with SharePoint, OneDrive, Teams, Yammer and Exchange and help organizations manage and govern information by ensuring content is kept only for a required time, and then permanently deleted.

Retention labels:

- Are applied at an item level.
- Emails and documents can have only a single retention label assigned to it at a time.
- Retention settings from retention labels travel with the content in your Microsoft 365 tenant.
- Can be applied manually or automatically.
- Retention labels support disposition review of the content before it's permanently deleted.

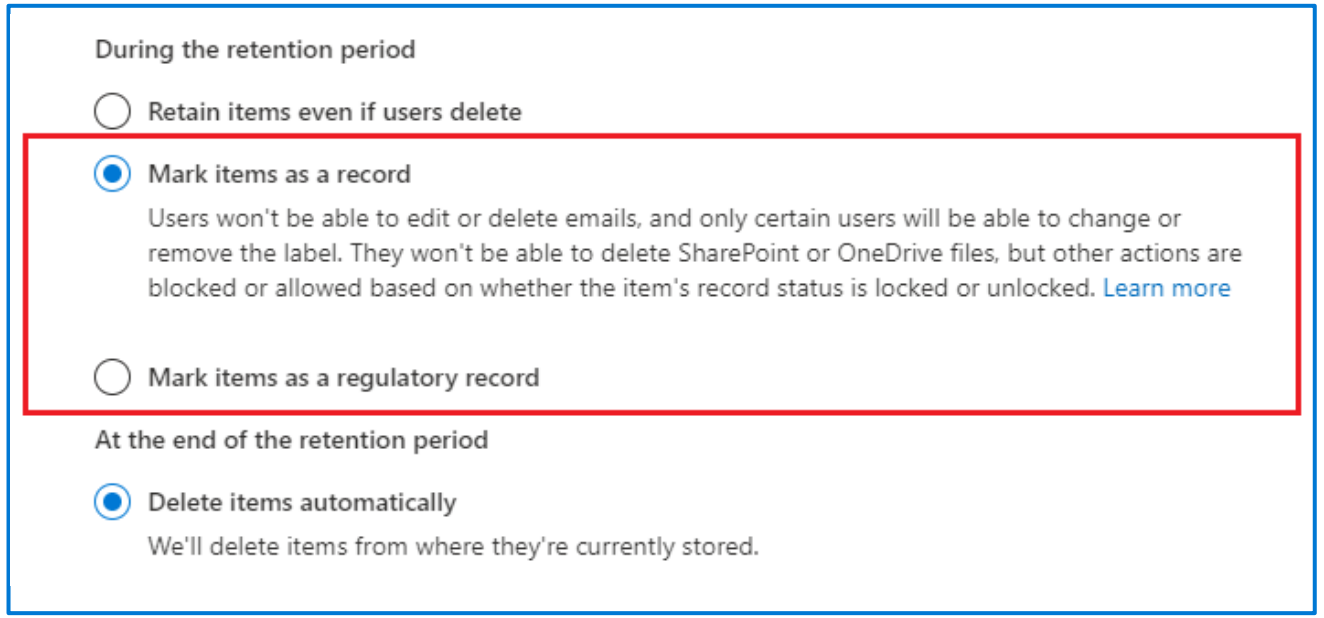
Retention policies:

- Are applied at site or mailbox level.
- Can be applied to multiple locations or specific locations or users.
- Items inherit the retention settings from their container.
- If an item is moved, the retention setting does not travel to the new location.

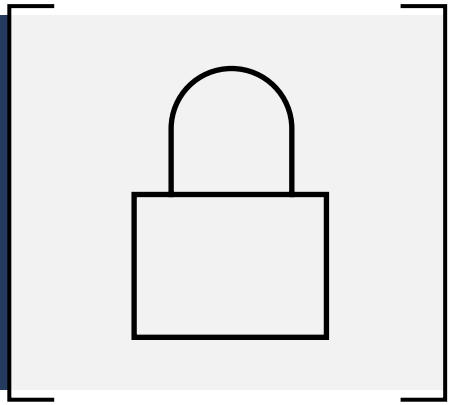
Records management

Records management helps an organization look after their legal obligations and helps to demonstrate compliance with regulations.

- When content is labeled as a record, the following happens:
  - Restrictions are put in place to block certain activities.
  - Activities are logged.
  - Proof of disposition is kept at the end of the retention period.
- To enable items to be marked as records, an administrator sets up retention labels.



Module 4: Describe insider risk capabilities in Microsoft Purview



Module 4 Introduction

After completing this module, you should be able to:

- Describe how Microsoft Purview can help organizations identify insider risks and take appropriate action.

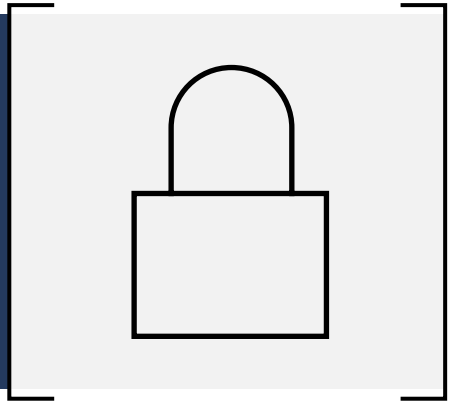
Insider risk solutions in Microsoft Purview

Insider risk management helps minimize internal risks by enabling you to detect, investigate, and act on malicious and inadvertent activities in your organization.

Communication compliance helps minimize communication risks by helping you detect, capture, and act on inappropriate messages in your organization. Supported services: Microsoft Teams, Exchange Online, Yammer, & 3rd party communications in an org.

Information barriers allow you to restrict communication and collaboration between two internal groups to avoid a conflict of interest from occurring in your organization. Supported in Microsoft Teams, OneDrive for Business, SharePoint Online, and more.

Module 5: Describe eDiscovery & Audit capabilities in Microsoft Purview



Module 5 Introduction

After completing this module, you should be able to:

- Describe the eDiscovery capabilities of Microsoft Purview.
- Describe the auditing capabilities of Microsoft Purview.

eDiscovery in Microsoft Purview

- Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic information that can be used as evidence in legal cases.
- eDiscovery tools: Content search, eDiscovery (Standard), eDiscovery (Premium)

Content search	eDiscovery (Standard)	eDiscovery (Premium)
▪ Search for content ▪ Keyword queries and search conditions ▪ Export search results ▪ Role-based permissions	▪ Search and export ▪ Case management ▪ Legal hold	▪ Custodian management ▪ Legal hold notifications ▪ Advanced indexing ▪ Review set filtering ▪ Tagging ▪ Analytics ▪ Predictive coding models ▪ And more...

Auditing in Microsoft Purview

- Microsoft Purview auditing solutions help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations.
- Microsoft Purview provides two auditing solutions: Audit (Standard) and Audit (Premium).

Audit (Standard)

Log and search for audited activities:

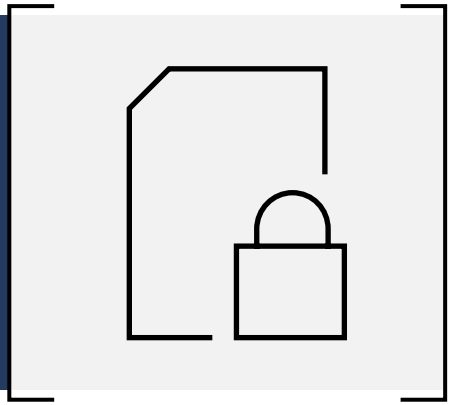
- Enabled by default
- Thousands of audited events
- 90-day audit record retention
- Accessed by GUI, cmdlet, and API

Audit (Premium)

Advanced Audit capabilities:

- Longer retention of audit records
- Custom audit retention policies
- High-value, crucial events
- Higher bandwidth access to API

Module 6: Describe resource governance capabilities in Azure



Module 6 Introduction

After completing this module, you should be able to:

- Describe Azure Policy.
- Describe Azure Blueprints.
- Describe the capabilities of the Microsoft Purview governance portal.

Azure Policy

Region
SKU
Tags

Policy — Definition (json) — Effect (Deny, Audit) — Scope

Trigger a Policy evaluation

- In-scope resource is created, deleted, or updated.
- A policy or an initiative is newly assigned to a scope.
- A policy or an initiative assigned to a scope is updated.
- The standard compliance evaluation cycle.

Azure Policy

- Help enforce standards and assess compliance across your organization.
- A compliance dashboard, to evaluate the overall state of the environment.
- Evaluates resources in Azure and Arc enabled resources.

Responses to non-compliant resources

- Deny a change to a resource.
- Log changes to a resource.
- Alter a resource before or after a change.
- Deploy related compliant resources.

Microsoft Security

Demo

Azure policy

Azure Blueprints

Preview!

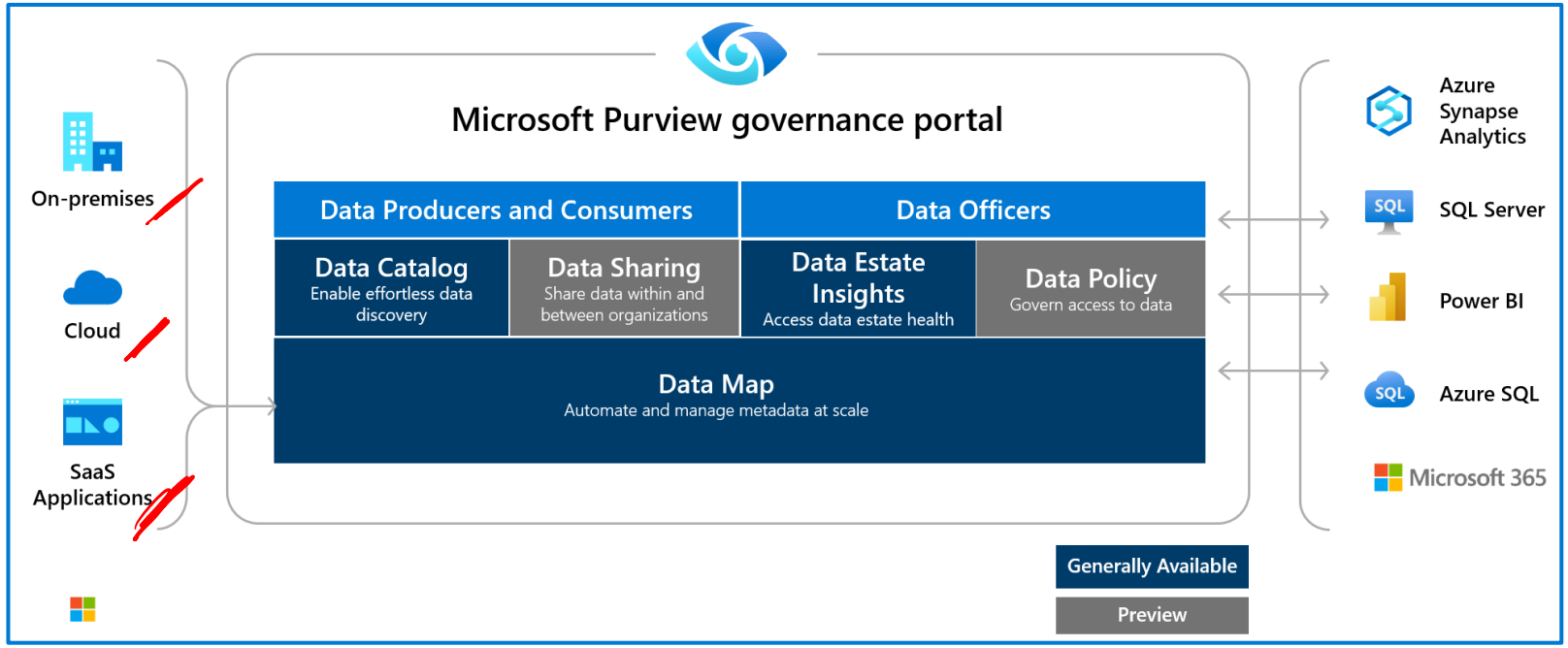
- Azure Blueprints provide a way to define a repeatable set of Azure resources.
- Rapidly provision environments, that are in line with the organization's compliance requirements.
- Provision Azure resources across several subscriptions simultaneously for quicker delivery.
- Declarative way to orchestrate the deployment of various resource templates and artifacts, including:
  - Role Assignments
  - Policy Assignments
  - Azure Resource Manager templates (ARM templates)
  - Resource Groups
- Blueprint objects are replicated to multiple Azure regions.
- The relationship between the blueprint definition and the blueprint assignment is preserved.

Bicep → json Infra as Code

Microsoft Purview governance portal

The ***Microsoft Purview governance portal*** provides a unified data governance service that helps organizations manage and govern their on-premises, multi-cloud, and SaaS data.

- Data Map - identify and classify sensitive data.
- Data Catalog - quickly and easily find relevant data.
- Data Estate Insights – know where sensitive data is, and how it moves.
- Data Sharing (preview) – share data within and between organizations.
- Data Policy (preview) – govern data access



Learning Path Summary

In this learning path, you have:

- Learned about the Service Trust Portal and privacy with Microsoft.
- Learned about the compliance management capabilities in Microsoft Purview, including the compliance portal, Compliance Manager, and Compliance Score.
- Learned about the information protection and data lifecycle management capabilities of Microsoft Purview, including sensitivity & retention labels, DLP, and more.
- Learned about insider risk capabilities in Microsoft Purview.
- Learned about eDiscovery & audit capabilities of Microsoft Purview.
- Describe resource governance capabilities in Azure, including Azure policy, Blueprints, and the Microsoft Purview governance portal.

Microsoft Security