Microsoft

Swiss Post
Cybersecurity

Introduction to Microsoft Priva and Microsoft Purview

Microsoft
Solutions Partner
Security
Specialist
Threat Protection

Learning path agenda

- Describe Microsoft's Service Trust Portal and the privacy capabilities of Microsoft Priva.
- Describe the data security solutions of Microsoft Purview.
- Describe the data compliance solutions of Microsoft Purview.
- Describe the data governance solutions of Microsoft Purview.

Describe Microsoft's Service Trust portal and privacy capabilities

Module 1 introduction

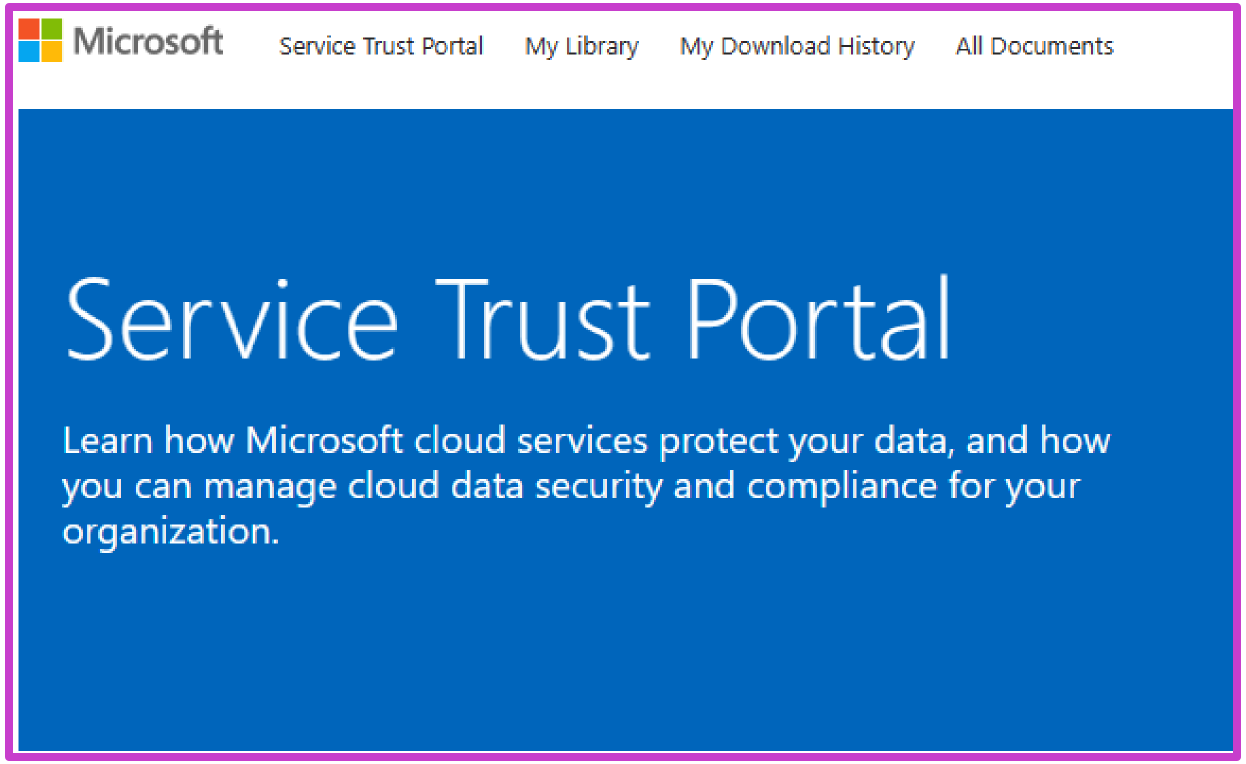
After completing this module, you should be able to:

1. Describe the offerings of the Service Trust Portal.
2. Describe Microsoft’s privacy principles.
3. Describe Microsoft Priva.

Microsoft Service Trust Portal

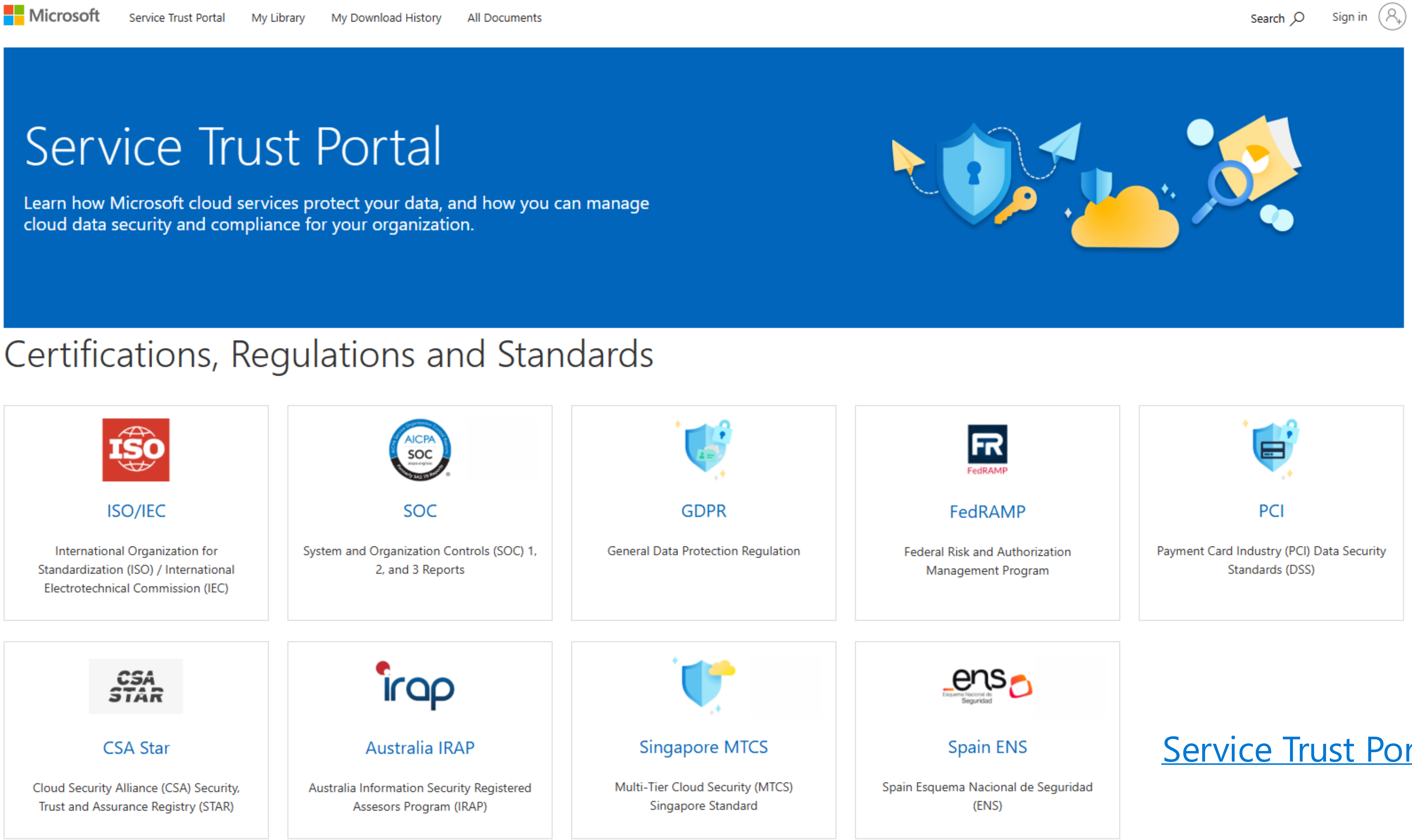
Microsoft's site for publishing audit reports and other compliance-related information associated with Microsoft's cloud services.

- Certifications, regulations and standards.
- Reports, white papers and artifacts.
- Industry and regional resources.
- Resources for your organization.



Service Trust Portal

Learn how Microsoft cloud services protect your data, and how you can manage cloud data security and compliance for your organization.



Service Trust Portal

Learn how Microsoft cloud services protect your data, and how you can manage cloud data security and compliance for your organization.

Certifications, Regulations and Standards

ISO/IEC

International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)

SOC

System and Organization Controls (SOC) 1, 2, and 3 Reports

GDPR

General Data Protection Regulation

FedRAMP

Federal Risk and Authorization Management Program

PCI

Payment Card Industry (PCI) Data Security Standards (DSS)

CSA Star

Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR)

Australia IRAP

Australia Information Security Registered Assesors Program (IRAP)

Singapore MTCS

Multi-Tier Cloud Security (MTCS) Singapore Standard

Spain ENS

Spain Esquema Nacional de Seguridad (ENS)

[Service Trust Portal Home Page]

Demo

Service Trust Portal

Microsoft’s privacy principles

1. **Control:** Putting you, the customer, in control of your privacy with easy-to-use tools and clear choices.
2. **Transparency:** Being transparent about data collection and use so that everyone can make informed decisions.
3. **Security:** Protecting the data that’s entrusted to Microsoft by using strong security and encryption.
4. **Strong legal protections:** Respecting local privacy laws and fighting for legal protection of privacy as a fundamental human right.
5. **No content-based targeting:** Not using email, chat, files, or other personal content to target advertising.
6. **Benefits to you:** When Microsoft does collect data, it’s used to benefit you, the customer, and to make your experiences better.

Microsoft Priva

Helps organizations safeguard personal data and build a privacy-resilient workplace.

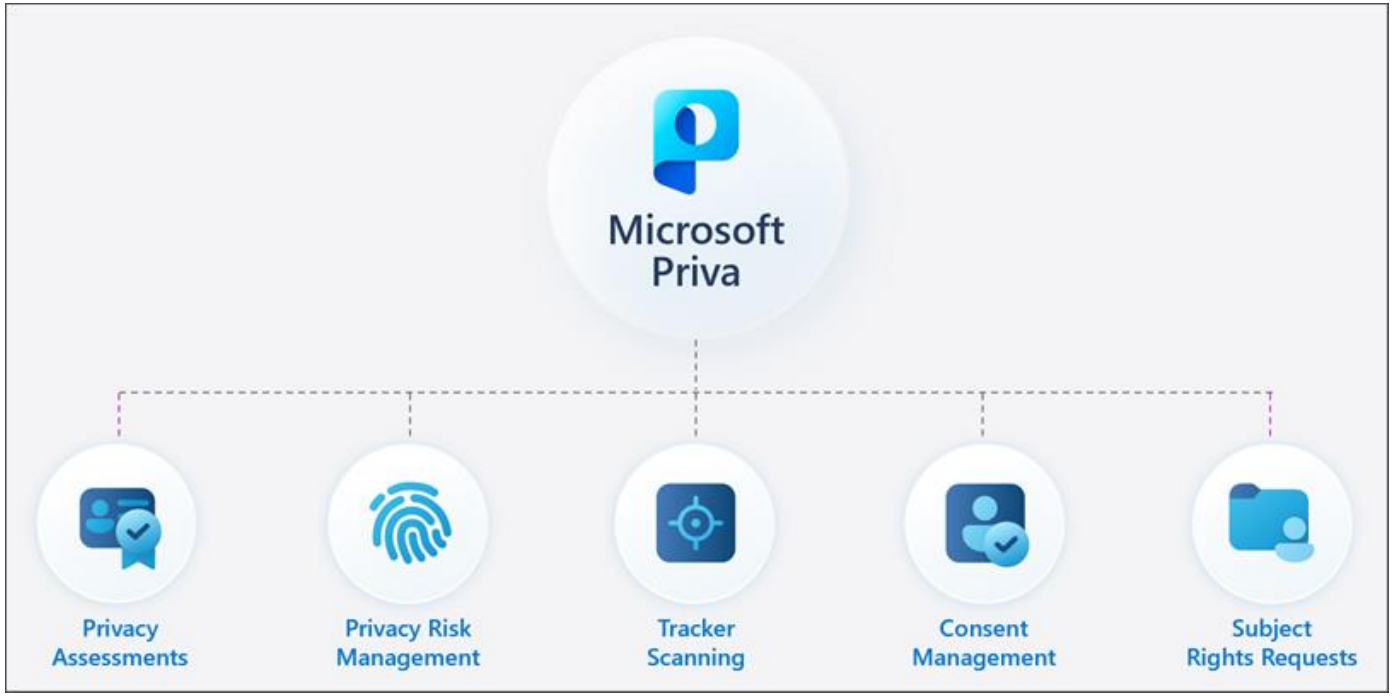
Privacy Risk Management: Visibility into your organization’s data and policy templates for reducing risks.

Subject Rights Requests: Automation and workflow tools for fulfilling data requests.

Consent Management: Effectively track consumer consent across their entire data estate.

Tracker Scanning: Automate the identification of tracking technologies across multiple web properties, driving website privacy compliance.

Privacy Assessments: Automates the discovery, documentation, and evaluation of personal data use across your entire data estate.



Module 2: Describe the data security solutions of Microsoft Purview

Module 2 introduction

After completing this module, you should be able to:

1 Describe how Microsoft Purview Information Protection helps organizations discover, classify, and protect sensitive information.

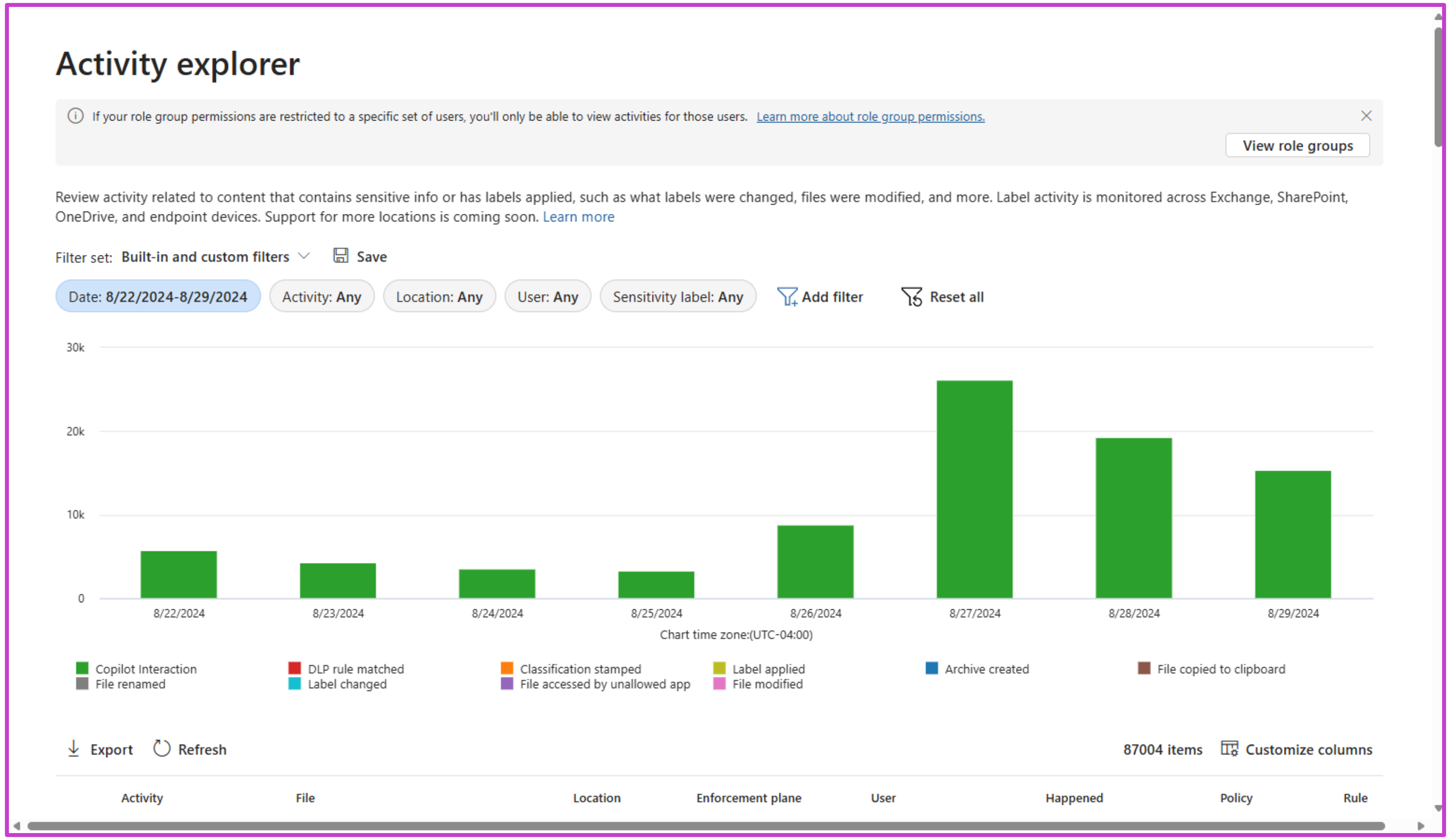
2 Describe how Microsoft Purview Data Loss Prevention helps organizations prevent their users from inappropriately sharing sensitive data with people who shouldn't have it.

3 Describe how Microsoft Purview Insider Risk Management helps minimize internal risks.

Data classification in Microsoft Purview Information Protection

Identify important information across the estate and ensure that data is handled in line with compliance requirements.

- Sensitive information types.
- Exact data match (EDM) classifiers
- Trainable classifiers: Pretrained classifiers and custom trainable classifiers.
- Content explorer: A snapshot of the items that have a sensitivity label, a retention label or have been classified as a sensitive information type
- Activity explorer: Monitor what's being done with labeled content across the organization.



Activity explorer

ⓘ If your role group permissions are restricted to a specific set of users, you'll only be able to view activities for those users. Learn more about role group permissions. ✕

View role groups

Review activity related to content that contains sensitive info or has labels applied, such as what labels were changed, files were modified, and more. Label activity is monitored across Exchange, SharePoint, OneDrive, and endpoint devices. Support for more locations is coming soon. Learn more

Filter set: Built-in and custom filters · Save

Date: 8/22/2024-8/29/2024 · Activity: Any · Location: Any · User: Any · Sensitivity label: Any · Add filter · Reset all

Export · Refresh · 87004 items · Customize columns

Activity	File	Location	Enforcement plane	User	Happened	Policy	Rule

Sensitivity labels and policies

Sensitivity labels are:

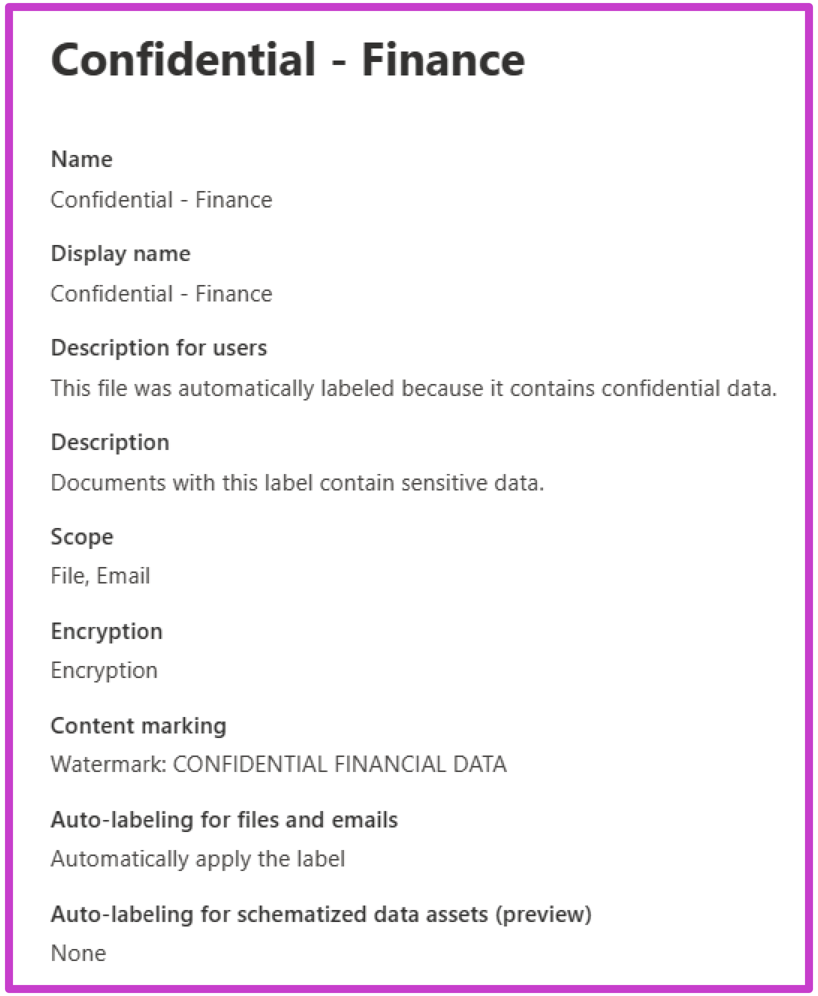
- Customizable
- Clear text
- Persistent

Sensitivity labels can:

- Encrypt
- Mark the content (watermark)
- Apply labels automatically
- Protect content in containers
- Extend to 3rd party apps/services
- Classify content w/o protection

Label policies

- 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.



Confidential - Finance

Name
Confidential - Finance

Display name
Confidential - Finance

Description for users
This file was automatically labeled because it contains confidential data.

Description
Documents with this label contain sensitive data.

Scope
File, Email

Encryption
Encryption

Content marking
Watermark: CONFIDENTIAL FINANCIAL DATA

Auto-labeling for files and emails
Automatically apply the label

Auto-labeling for schematized data assets (preview)
None

Data loss prevention (DLP)

Identify, monitor, and protect sensitive items across:

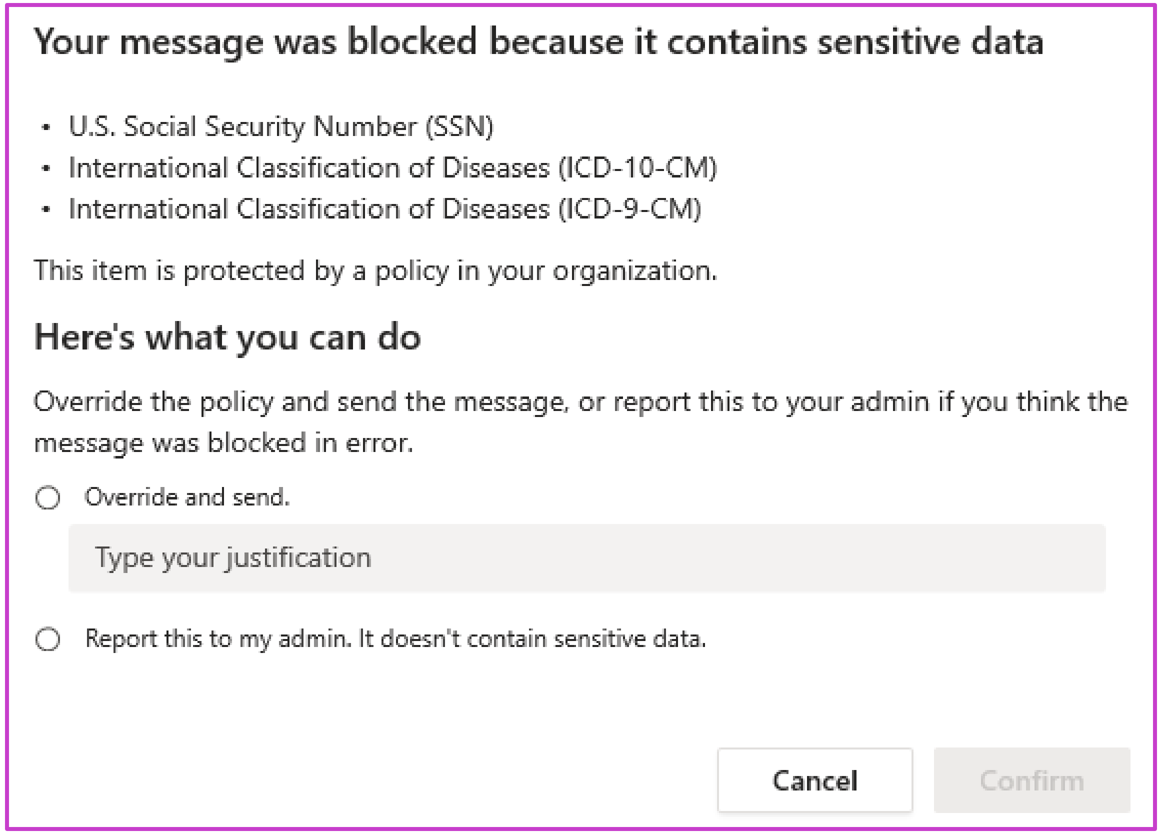
- Microsoft 365 services—OneDrive for Business, SharePoint Online, Exchange Online, and Office 365 applications.
- Microsoft Teams—Teams chat and channel messages.
- Devices —Windows 10, Windows 11, and macOS.
- Microsoft Defender for Cloud Apps.
- On-premises repositories.
- Power BI.

Protective actions DLP policies can take:

- Show a pop-up policy tip.
- Block sharing of sensitive items with or without override option.
- Move data at rest to a secure quarantine location.
- For Teams chat, sensitive information won't be displayed.

Security Copilot integration:

- Experience Copilot integration via the standalone and embedded experiences.
- Embedded experience supports summary of alerts.



Your message was blocked because it contains sensitive data

- U.S. Social Security Number (SSN)
- International Classification of Diseases (ICD-10-CM)
- International Classification of Diseases (ICD-9-CM)

This item is protected by a policy in your organization.

Here's what you can do

Override the policy and send the message, or report this to your admin if you think the message was blocked in error.

○ Override and send.

Type your justification

○ Report this to my admin. It doesn't contain sensitive data.

Microsoft Purview Insider Risk Management

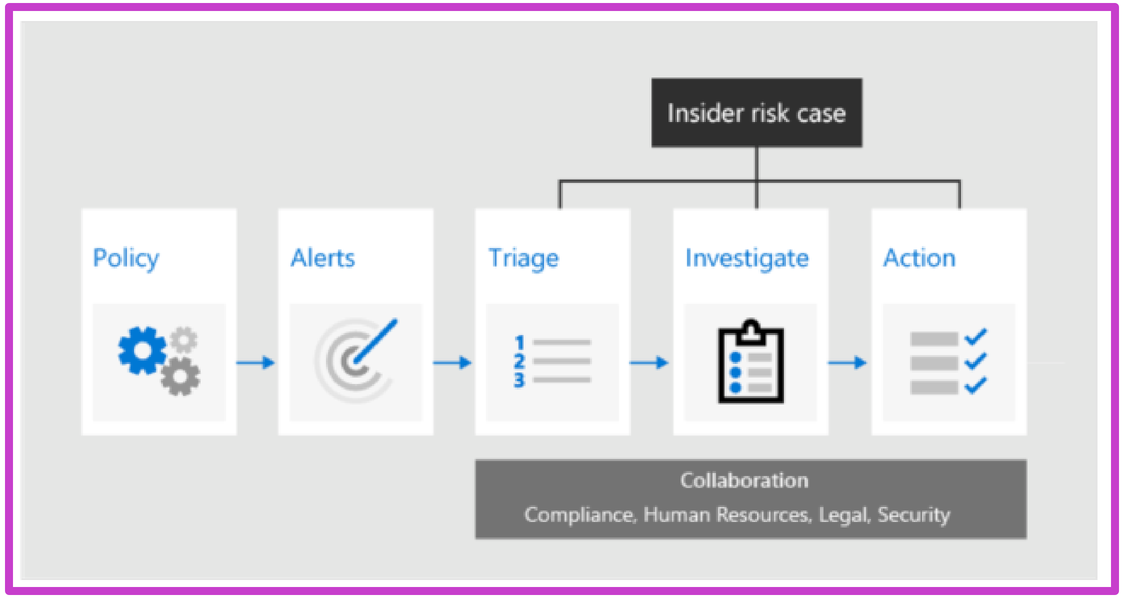
Helps organizations to identify, investigate, and address internal risks such as data leaks, intellectual property theft, fraud, insider trading, and more.

Insider risk management workflow:

- Create ***policies*** to define what risk indicators are examined.
- ***Alerts*** automatically generated by risk indicators that match policy conditions.
- ***Triage*** alerts with a needs review status.
- Cases are created for alerts that require deeper review and ***investigation***.
- Reviewers can quickly take ***action*** to resolve the case.

Security Copilot integration:

- Experience Copilot integration via the standalone and embedded experiences.
- Embedded experience supports summary of alerts.



Adaptive protection

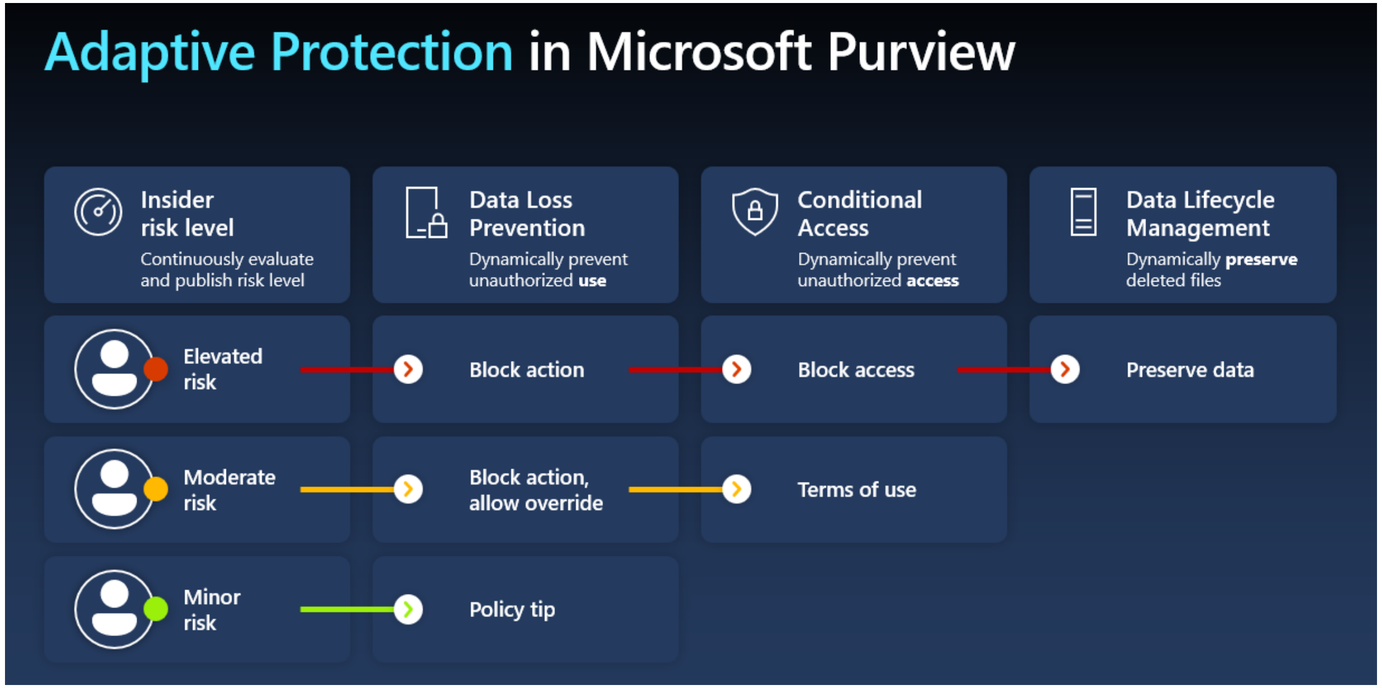
Adaptive protection in Microsoft Purview uses machine learning (ML) to identify the most critical risks and proactively and dynamically apply protection controls.

Based on risk in Insider Risk Management, Adaptive Protection in Microsoft Purview applies controls from:

- Data Loss Prevention
- Microsoft Purview Data Lifecycle Management (preview)
- Microsoft Entra Conditional Access (preview)

Mitigate potential risks by using:

- Context-aware detection.
- Dynamic controls
- Automated mitigation



Adaptive Protection in Microsoft Purview

Insider risk level Continuously evaluate and publish risk level	Data Loss Prevention Dynamically prevent unauthorized **use**	Conditional Access Dynamically prevent unauthorized **access**	Data Lifecycle Management Dynamically **preserve** deleted files
Elevated risk	Block action	Block access	Preserve data
Moderate risk	Block action, allow override	Terms of use	
Minor risk	Policy tip		

Module 3: Describe the data compliance solutions of Microsoft Purview

Module 3 introduction

After completing this module, you should be able to:

1. Describe Audit and eDiscovery in Microsoft Purview.
2. Describe Compliance Manager in Microsoft Purview.
3. Describe Communication Compliance in Microsoft Purview.
4. Describe Records Management in Microsoft Purview.

Microsoft Purview Audit

Help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations.

Audit (Standard)

Log and search for audited activities:

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

Audit (Premium)

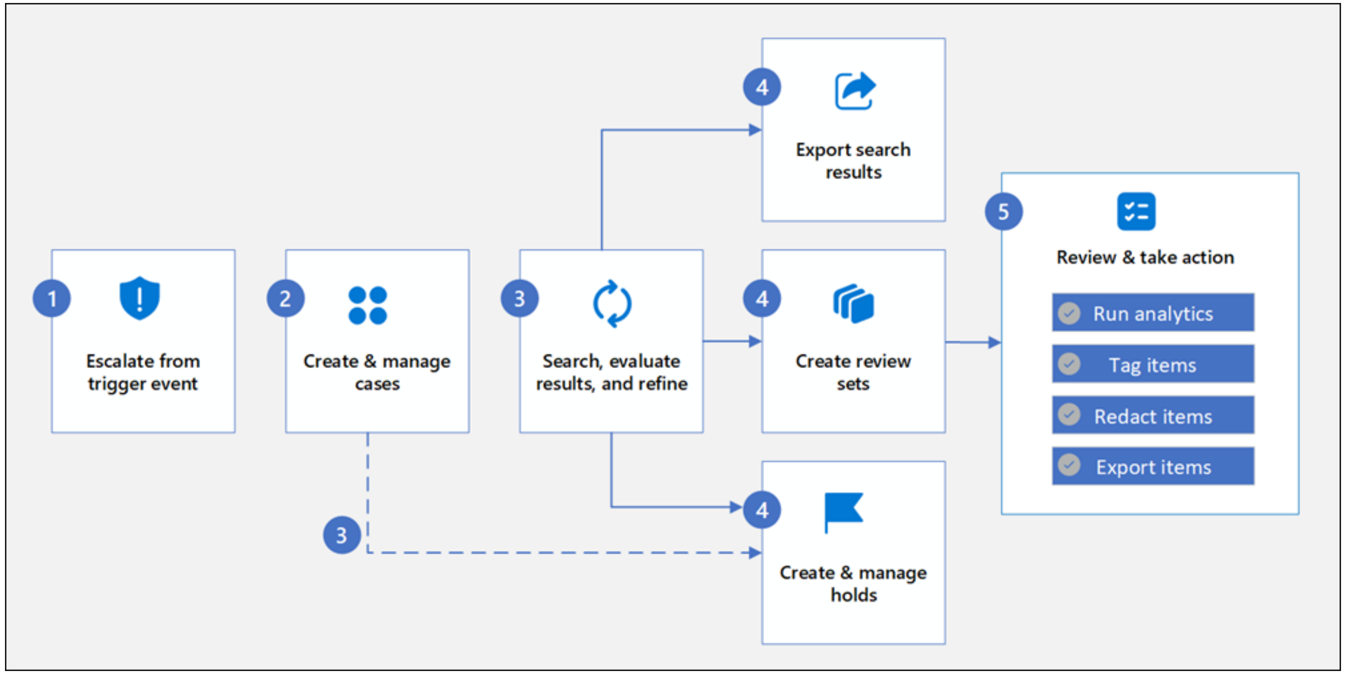
Builds on the capabilities of Audit (Standard) with:

- 1 year default retention period
- Customized retention policies
- Intelligent insights
- Higher bandwidth access to API

Microsoft Purview eDiscovery

The process of identifying and delivering electronic information that can be used as evidence in legal cases.

1. Trigger events prompt the creation of a new case in eDiscovery (preview).
2. Create & manage cases
3. Search the content locations in your organization, using built-in search tools.
4. Actions include: export search results, create review sets, create holds.
5. Review and take action from review sets, including: run analytics, tag items, export items.



Copilot integration with eDiscovery in the embedded experience – Summarize review sets and natural language to Keyword Query language (KeyQL) queries.

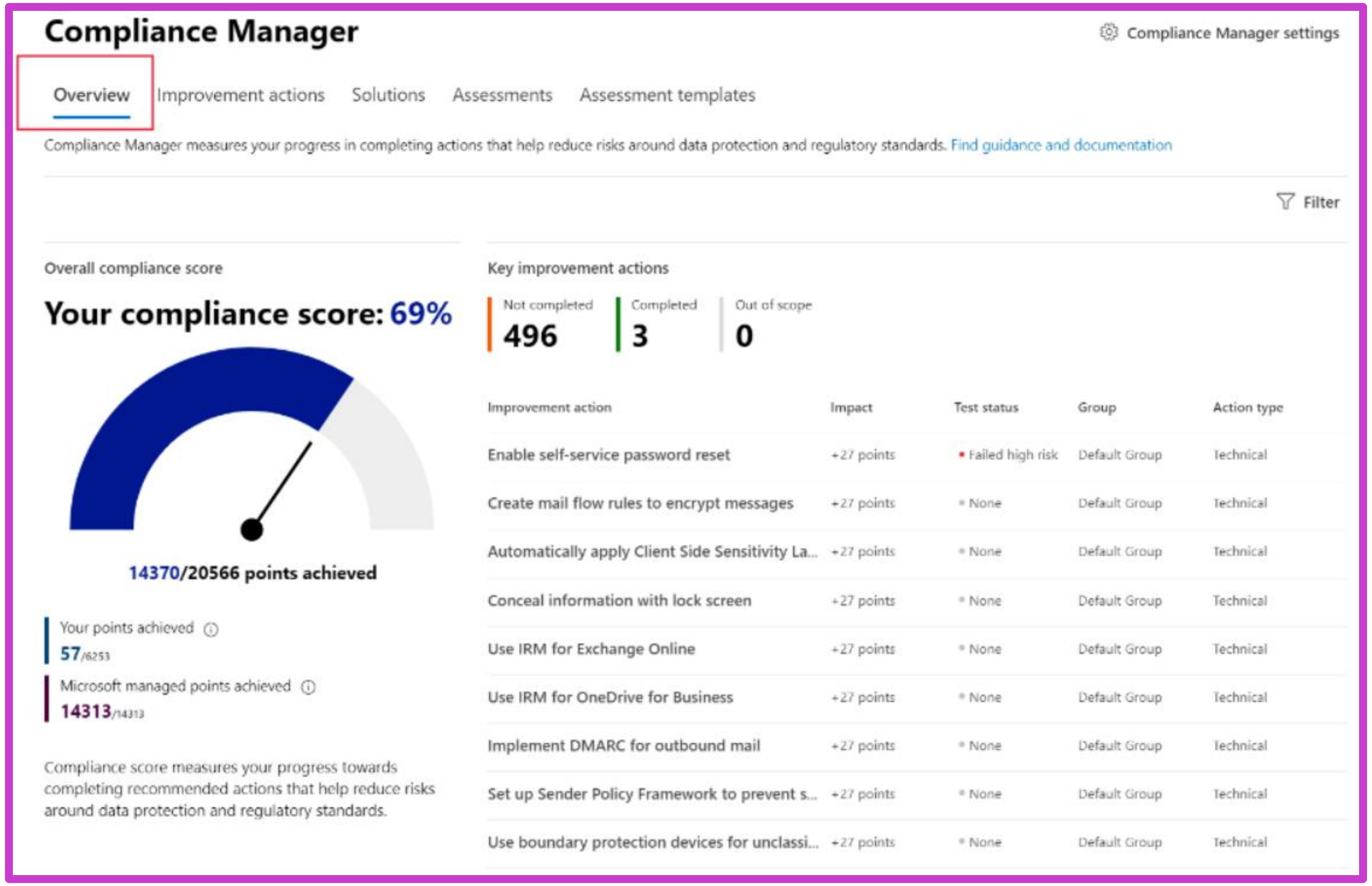
Compliance Manager

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 that shows overall compliance posture.

Key elements of Compliance Manager

- Controls
- Assessments
- Regulations
- Improvement actions



Compliance Manager measures your progress in completing actions that help reduce risks around data protection and regulatory standards. Find guidance and documentation

Overall compliance score

Your compliance score: 69%

14370/20566 points achieved

Your points achieved ⓘ
57/6253

Microsoft managed points achieved ⓘ
14313/14313

Compliance score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Key improvement actions

Not completed	Completed	Out of scope
496	3	0

Improvement action	Impact	Test status	Group	Action type
Enable self-service password reset	+27 points	● Failed high risk	Default Group	Technical
Create mail flow rules to encrypt messages	+27 points	● None	Default Group	Technical
Automatically apply Client Side Sensitivity La...	+27 points	● None	Default Group	Technical
Conceal information with lock screen	+27 points	● None	Default Group	Technical
Use IRM for Exchange Online	+27 points	● None	Default Group	Technical
Use IRM for OneDrive for Business	+27 points	● None	Default Group	Technical
Implement DMARC for outbound mail	+27 points	● None	Default Group	Technical
Set up Sender Policy Framework to prevent s...	+27 points	● None	Default Group	Technical
Use boundary protection devices for unclassi...	+27 points	● None	Default Group	Technical

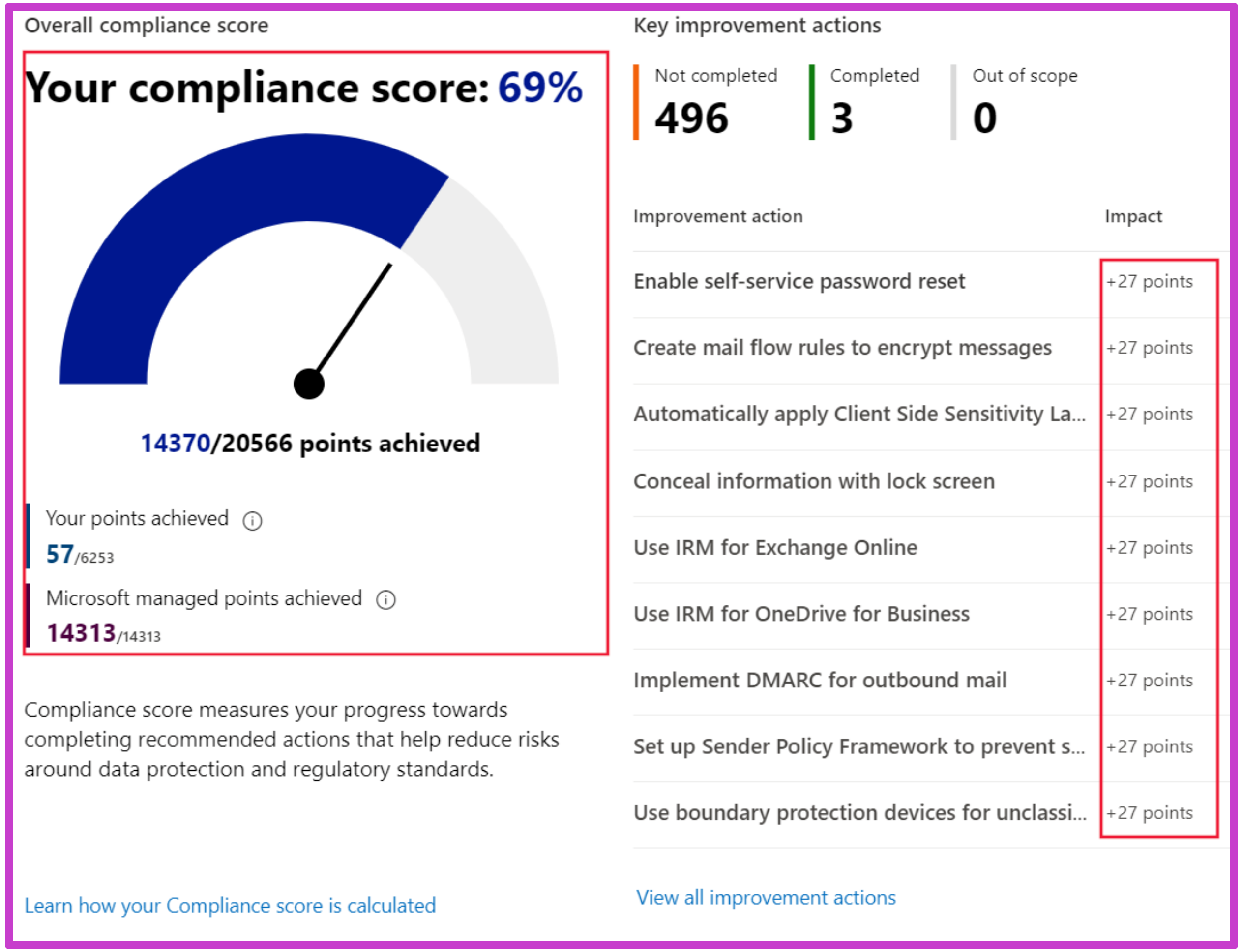
Compliance score

Benefits of compliance score:

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

Understand your compliance score

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



Overall compliance score

Your compliance score: 69%

14370/20566 points achieved

Your points achieved ⓘ
57/6253

Microsoft managed points achieved ⓘ
14313/14313

Compliance score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Learn how your Compliance score is calculated

Key improvement actions

Not completed	Completed	Out of scope
496	3	0

Improvement action	Impact
Enable self-service password reset	+27 points
Create mail flow rules to encrypt messages	+27 points
Automatically apply Client Side Sensitivity La...	+27 points
Conceal information with lock screen	+27 points
Use IRM for Exchange Online	+27 points
Use IRM for OneDrive for Business	+27 points
Implement DMARC for outbound mail	+27 points
Set up Sender Policy Framework to prevent s...	+27 points
Use boundary protection devices for unclassi...	+27 points

View all improvement actions

Data lifecycle management with retention labels and policies

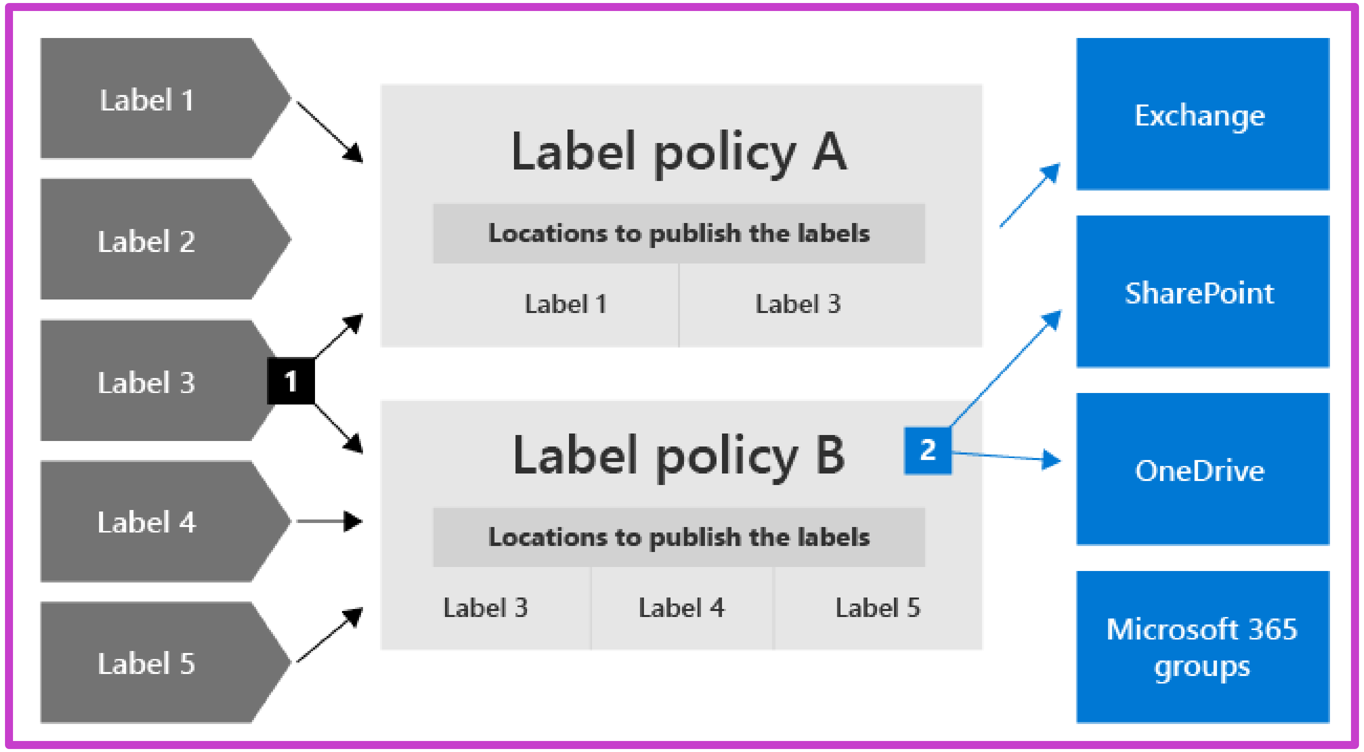
Manage and govern information by ensuring content is kept only for the required time.

Retention labels:

- Assigned at an item level.
- Only one label can be assigned at a time.
- Retention settings travel with the content.
- Can be applied automatically.
- Support disposition review.
- Published through label policy.

Retention policies:

- Assigned at a site level or mailbox level.
- A single policy can be applied to multiple locations, or to specific locations or users.
- Items inherit the retention settings from their container.



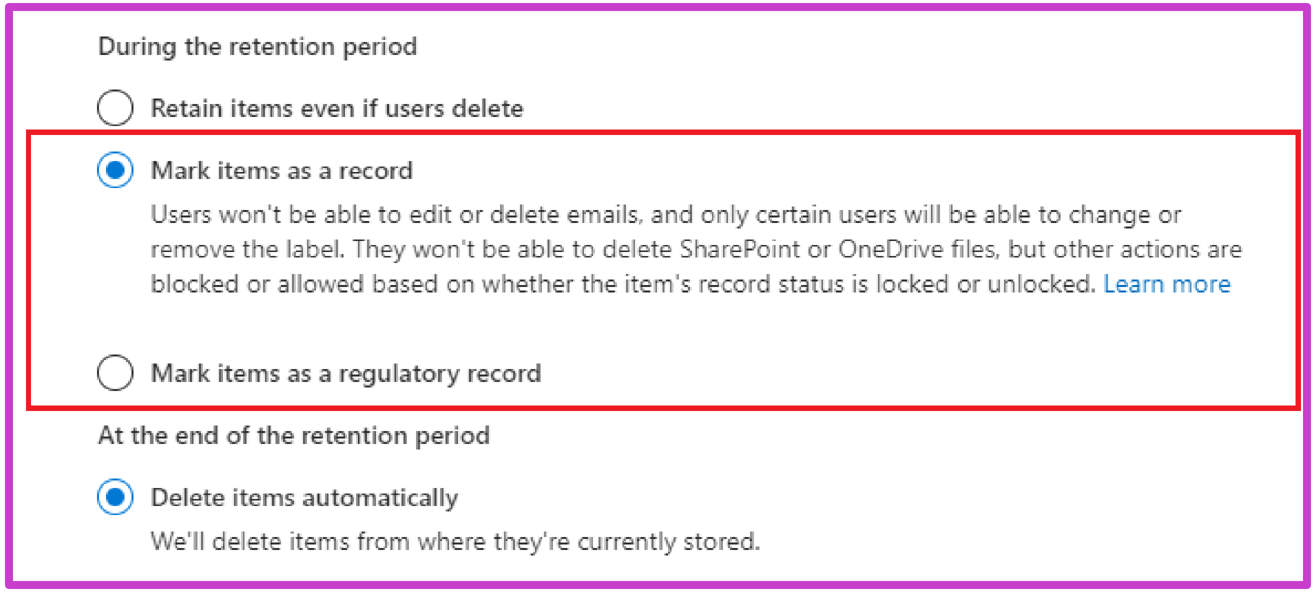
Records management

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

For content labeled as a record:

- 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.



During the retention period

○ Retain items even if users delete

● Mark items as a record

Users won't be able to edit or delete emails, and only certain users will be able to change or remove the label. They won't be able to delete SharePoint or OneDrive files, but other actions are blocked or allowed based on whether the item's record status is locked or unlocked. Learn more

○ Mark items as a regulatory record

At the end of the retention period

● Delete items automatically

We'll delete items from where they're currently stored.

Module 4: Describe the data governance solutions of Microsoft Purview

Module 4 introduction

After completing this module, you should be able to:

1. Describe benefits of data governance.
2. Describe key features of Microsoft Purview Data Catalog.

Benefits of data governance

- **For organization-wide data consumers:**
- Data discovery - helps you easily find the data you need.
- Secure access - facilitates safe access to your data.
- Data understanding - providing what you need to know about the data.

- **For data owners and stewards:**
- Data curation and management - helps you deliver high quality data that's easy to understand and safely access for organization-wide applications.
- Responsible data use - helps you ensure that your data is used by intended users for intended purposes.
- Impact analysis - understand actions on the data that may impact your data.

- **For data officers and CxO stakeholders:**
- Data value creation - maximize value creation from your data while reducing operations spend.
- Data estate standardization - create common controls across your data estate with federated accountability so your data is healthy and safe.

Data Consumers

Quickly find and use relevant, trusted datasets through streamlined access request workflow.

Data Owners

Register data assets for use, manage classifications and access, and ensure high quality standards.

Data Stewards

Ensure data quality, seamless data discovery, glossary consistency, and lineage.

Central Data Office

Establish and ensure governance policies, active metadata, compliance, and insights into overall governance health.

Microsoft Purview Data Catalog

The goal of Microsoft Purview Data Catalog is to provide a platform for data governance and to drive business value creation in your organization.

- Organize data with **business domains** (sales, finance, etc.) that make data familiar and accessible and set objectives and key results (OKRs) to link business objectives to the data catalog.
- Group related assets into **data products** so users can easily find the full data picture.
- Define **critical data elements** and attach rules and policies that feed into **self-service data access**, ensuring users have access to the right data.
- Enable **data discovery** across the business with search and browse capabilities—with additional efficiencies offered by Copilot in Purview for simple, fast interaction.

Learning path summary

Describe the capabilities of Microsoft compliance solutions.

In this learning path, you have:

- Learned about Microsoft's Service Trust Portal and the privacy capabilities of Microsoft Priva.
- Learned about the data security solutions of Microsoft Purview.
- Learned about the data compliance solutions of Microsoft Purview.
- Learned about the data governance solutions of Microsoft Purview.

Knowledge check

Privacy and how private data is handled are top concerns for organizations and consumers. Microsoft helps organizations meet these challenges, through capabilities offered through two solutions. What are those solutions?

A. Microsoft Purview eDiscovery and Microsoft Purview Audit.

B. Priva Privacy Risk Management and Priva Subject Rights Requests.

C. Microsoft Purview Insider Risk Management and Microsoft Purview Communication Compliance.

Your new colleagues on the admin team are unfamiliar with the concept of shared controls in Compliance Manager. How would the concept of shared controls be explained?

A. Controls that both external regulators and Microsoft share responsibility for implementing.

B. Controls that both your organization and external regulators share responsibility for implementing.

C. Controls that both your organization and Microsoft share responsibility for implementing.

Knowledge check continued

Within the organization, some emails are confidential and should be encrypted so that only authorized users can read them. How can this requirement be implemented?

A. Use the content explorer.
B. Use sensitivity labels.
C. Use records management.

The compliance admin for the organization wants to explain the importance of insider risk management, to the business leaders. What use case would apply?

A. To identify and protect against risks like an employee sharing confidential information.
B. To identify and protect against malicious software across your network, such as ransomware.
C. To identify and protect against devices shutting down at critical moments.