



NAME: STEPHEN KYALO -ADC-DP01-25005

PROGRAM: DATA PROTECTION SPECIALIST

CLOUD SLICE TOPIC: CAPABILITIES OF MICROSOFT COMPLIANCE SOLUTION

EXECUTIVE SUMMARY

Microsoft offers a comprehensive suite of services and cloud apps through its Microsoft Purview platform to aid organisations manage risk, protect sensitive data, and ensure regulatory compliance across hybrid and cloud environments. The Purview platform offers services such as Data Loss Prevention, Insider Risk Management, Records Management, Information Protection, Compliance Manager, Communication Compliance, eDiscovery and Audit, Risk and Compliance Integrations, and Regulatory and Industry Certifications.

A few of these services are explored in the labs provided and their capabilities document in the chapters that follow.

GLOSSARY

ISO/IEC - International Organisation for Standards / International Electrotechnical Commission

SOC 1 - System and Organisational Controls

HIPAA- Health Insurance Portability and Accountability Act

GDPR - General Data Protection Regulation

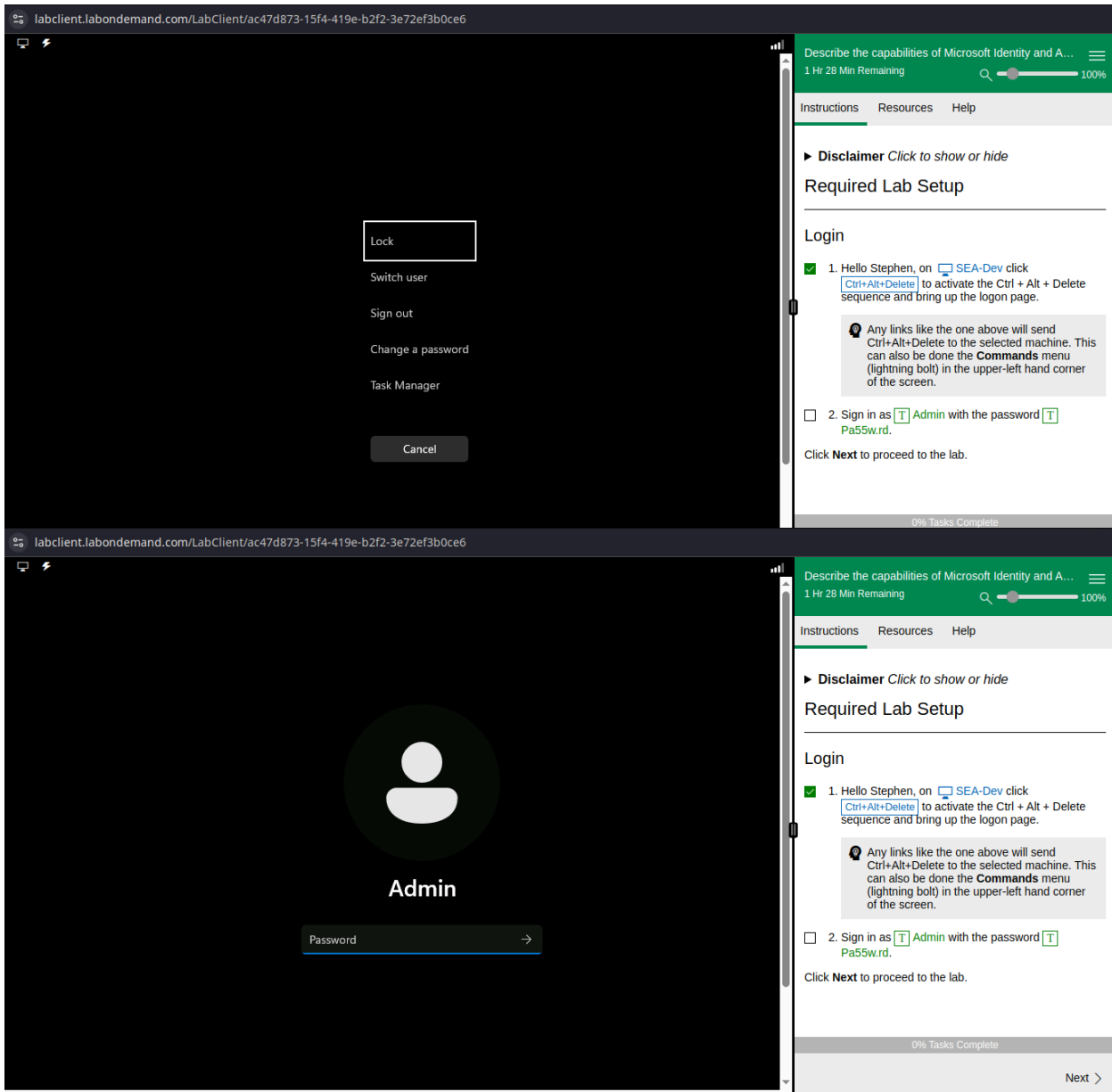
PCI DSS- Payment Card Industry Data Security Standard

RBA - Role Based Access

EXECUTIVE SUMMARY.....	2
GLOSSARY.....	2
1. LAB SETUP.....	3
2. EXPLORE THE SERVICE TRUST PORTAL.....	5
3. EXPLORE THE MICROSOFT PURVIEW PORTAL AND COMPLIANCE MANAGER.....	6
4. EXPLORE SENSITIVITY LABELS IN MICROSOFT PURVIEW.....	8
5. EXPLORE INSIDER RISK MANAGEMENT IN MICROSOFT PURVIEW.....	9
6. EXPLORE eDISCOVERY.....	9

1. LAB SETUP

Upon launching the cloud slice, the user is required to log out of the default account and log in with the provided **ADMIN** account and **PASSWORD**, as shown on the attached screenshots.



2. EXPLORE THE SERVICE TRUST PORTAL

The Microsoft Service Trust Portal is a centralised platform that provides access to Microsoft's compliance and trust-related documentation, tools, and resources. This helps organisations understand how Microsoft protects customer data and complies with regulatory standards.

Key features are:

- Industry and regional resources- compliance resources tailored to specific industries and regions.
- Resources for your org- documents specific to your organisation's Microsoft services, subscriptions and permissions.
- Certifications, Regulations and Standards- different global standards Microsoft is compliant with, eg PCI DSS, ISO/IEC, HIPAA, SOC 1, GDPR, among others
- Reports, Whitepapers and Artefacts- third-party audit and assessment reports on Microsoft compliance, in-depth whitepaper documents authored by Microsoft explaining security architecture, privacy controls, and regulatory alignment.

For future reference and updates, users can save the different documents to their library in the STP.

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

Describe the capabilities of Microsoft ... 1 Hr 19 Min Remaining

Instructions Resources Help

content available from the Service Trust Portal. You'll also visit the Trust Center to view information about Privacy at Microsoft.

Estimated Time: 10-15 minutes

Task 1

In this task, you'll explore the Service Trust portal and the different types of content available, you'll learn how to access reports, and how to save reports to your library.

- ☐ 1. Open Microsoft Edge.
- ☐ 2. In the address bar, enter aka.ms/STP. This will bring you to the landing page for the Service Trust Portal. The Service Trust Portal contains details about Microsoft's implementation of controls and processes that protect our cloud services and the customer data therein.
- ☐ 3. To access some of the resources on the Service Trust Portal, you must

0% Tasks Complete

< Previous Next >

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

FedRAMP

Describe the capabilities of Microsoft ... 1 Hr 4 Min Remaining

Instructions Resources Help

see all the available regions and countries. Select the tile for any country to view the applicable documents.

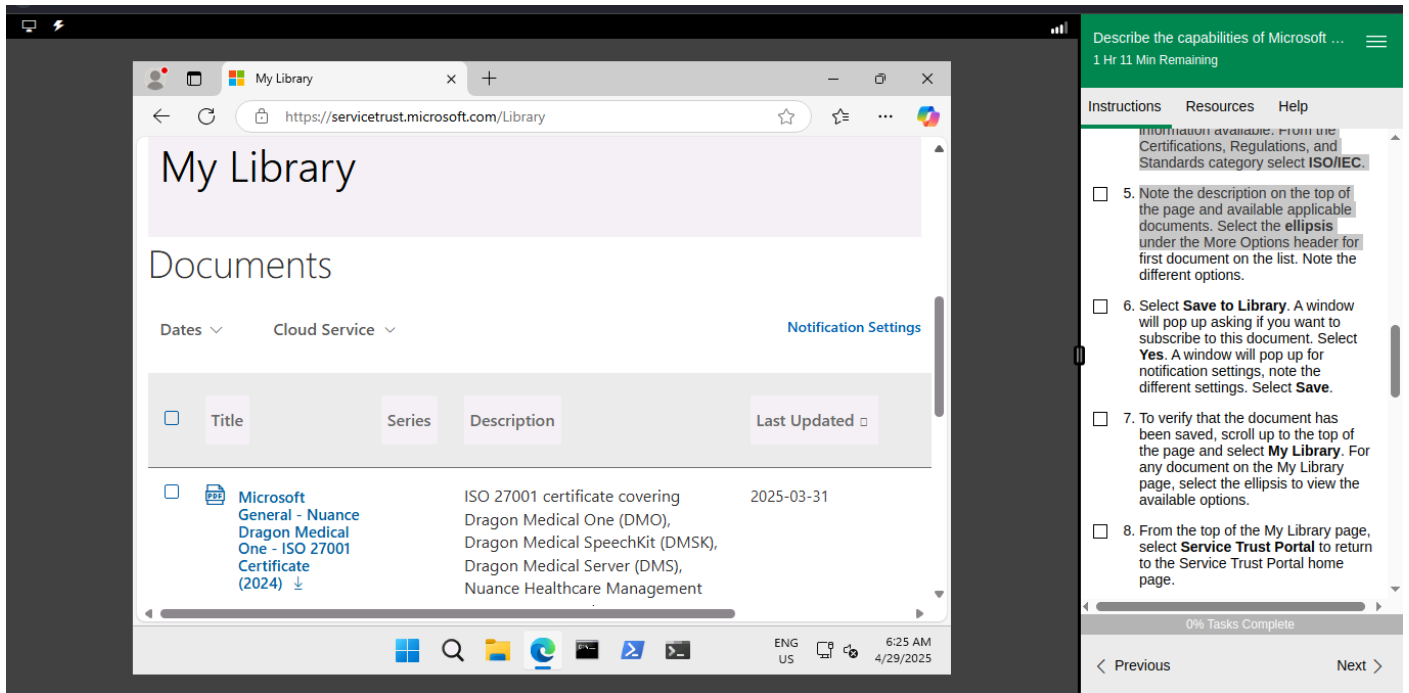
- ☐ 10. To return the Service Trust Portal home page, select the link **Service Trust Portal** at the top of the page.
- ☐ 11. From the Service Trust Portal home page, scroll down to the **Resource for your Organization** category. Select **Resources for your Organization**. Note that any documents listed here are based on your organization's subscription and permissions.
- ☐ 12. To return the Service Trust Portal home page, select the link **Service Trust Portal** at the top of the page.

Task 2

In this task, you'll visit the Trust Center and navigate to information that describes Privacy at Microsoft.

0% Tasks Complete

< Previous Next >

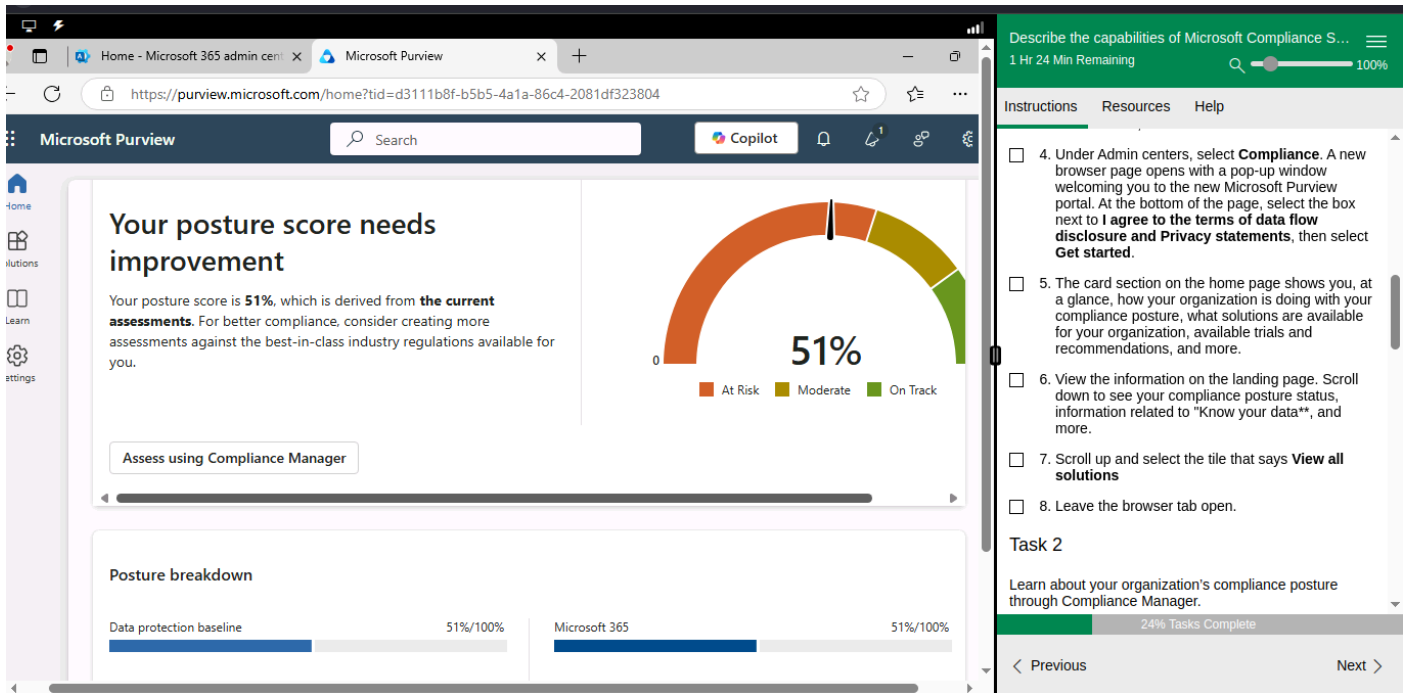


3. EXPLORE THE MICROSOFT PURVIEW PORTAL AND COMPLIANCE MANAGER

Microsoft Purview is Microsoft's unified data governance and compliance solution that includes both Microsoft Purview Portal and Compliance Manager to help organisations protect their data, manage risk, and meet regulatory requirements.

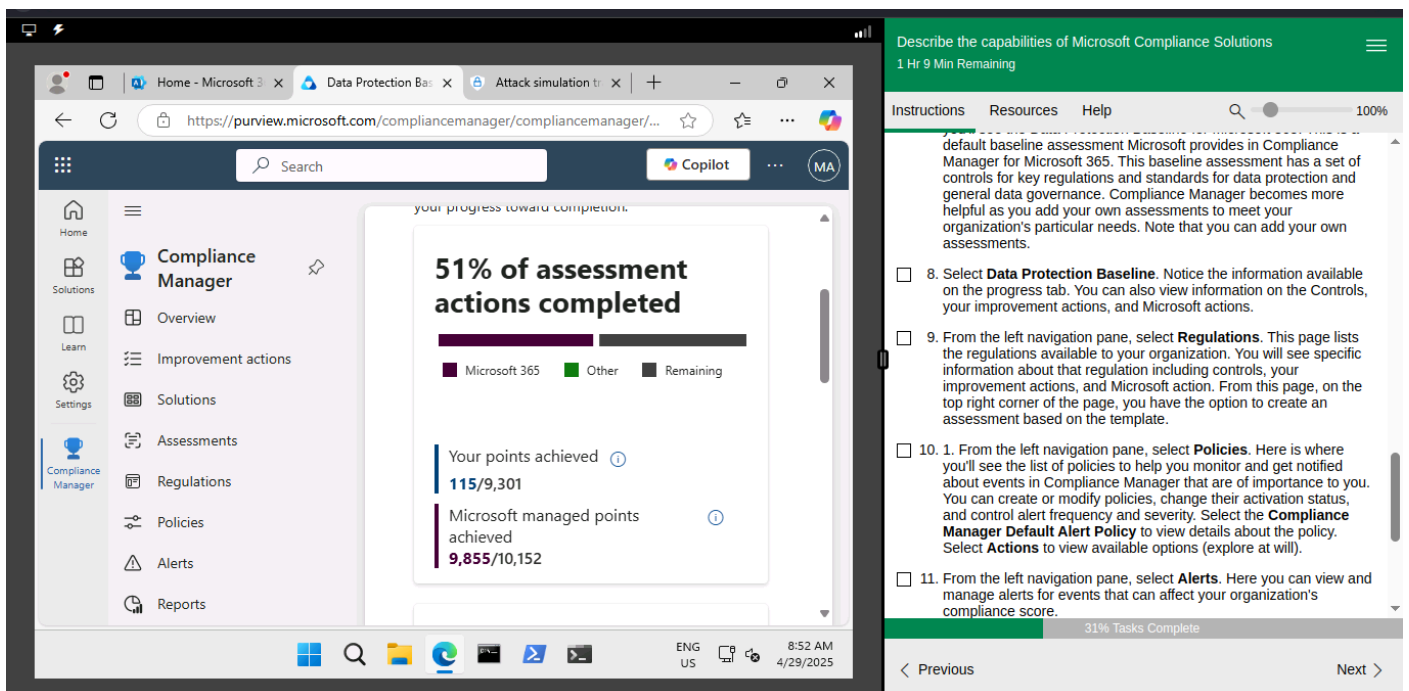
Microsoft Purview Portal is a centralised dashboard for managing compliance, privacy, and risk solutions across Microsoft services. Its capabilities include:

- Communication compliance- monitors and manages risky communication to ensure appropriate workplace behaviour.
- Records Management- classify, retain, and dispose business critical records securely.
- Data loss protection- define and enforce policies to prevent accidental data leaks.
- Information protection- apply labels and encryption to classify and protect sensitive content.
- Audit- get comprehensive logs of user and admin activities across services.



Compliance manager helps organisations manage their compliance posture against industry standards and regulations. The compliance manager analyses an organisations compliance posture and presents it as a compliance score value. Key features include:

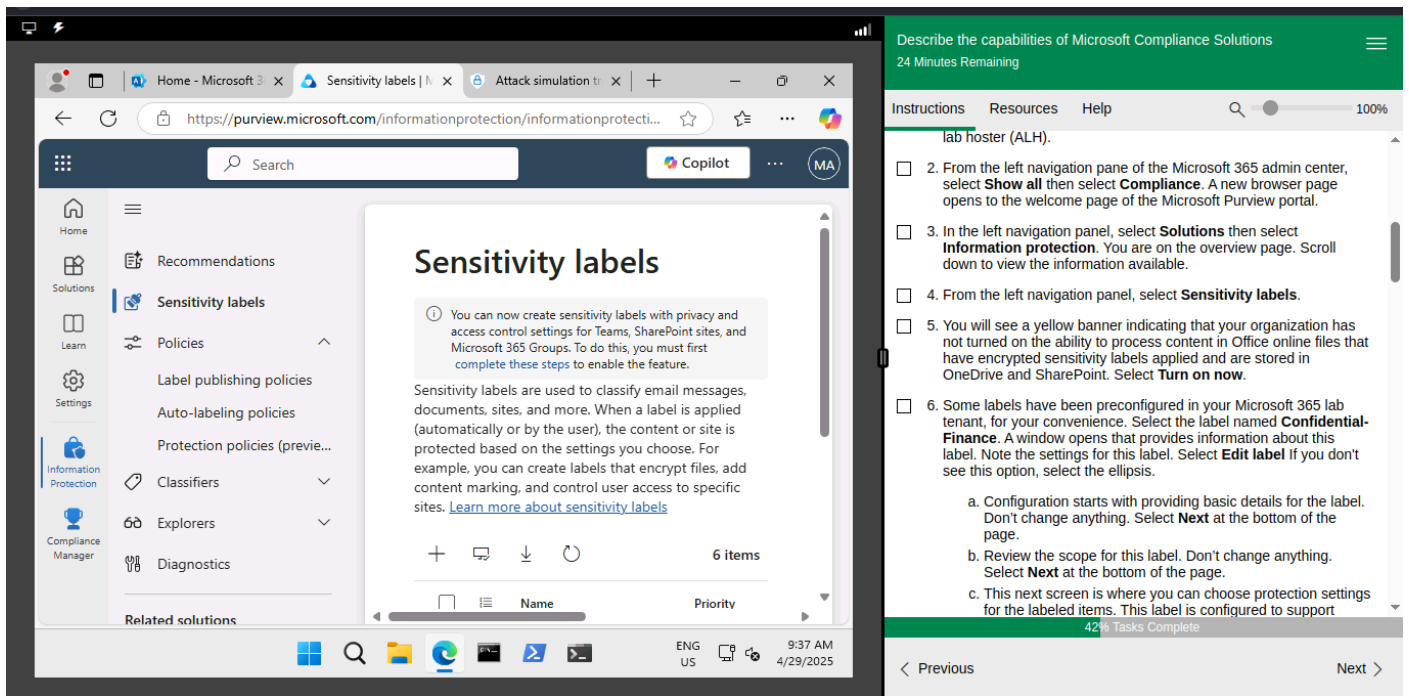
- Assessment Templates for 365 regulations
- Control Mapping responsibilities between Microsoft and the Customer.
- Improvement actions



4. EXPLORE SENSITIVITY LABELS IN MICROSOFT PURVIEW

Sensitivity labels are tags that are used to classify emails, files, documents, sites and more. They define Classification level(e.g. Confidential, Public, Internal), Protection settings such as Encryption, Watermarking, Access Restrictions and Content Marking.

Sensitivity labels move with the content they are applied to, ensuring persistent protection no matter where the content is moved or goes.



The screenshot shows the Microsoft Purview Sensitivity Labels page. The left navigation pane includes sections like Home, Solutions, Learn, Settings, Information Protection, and Compliance Manager. The main content area is titled 'Sensitivity labels' and includes a description of how to create and use sensitivity labels. A table below the text shows 6 items with columns for Name and Priority. The right sidebar contains instructions for the lab, starting with 'lab hoster (ALH)' and listing steps 2 through 6.

Describe the capabilities of Microsoft Compliance Solutions
24 Minutes Remaining

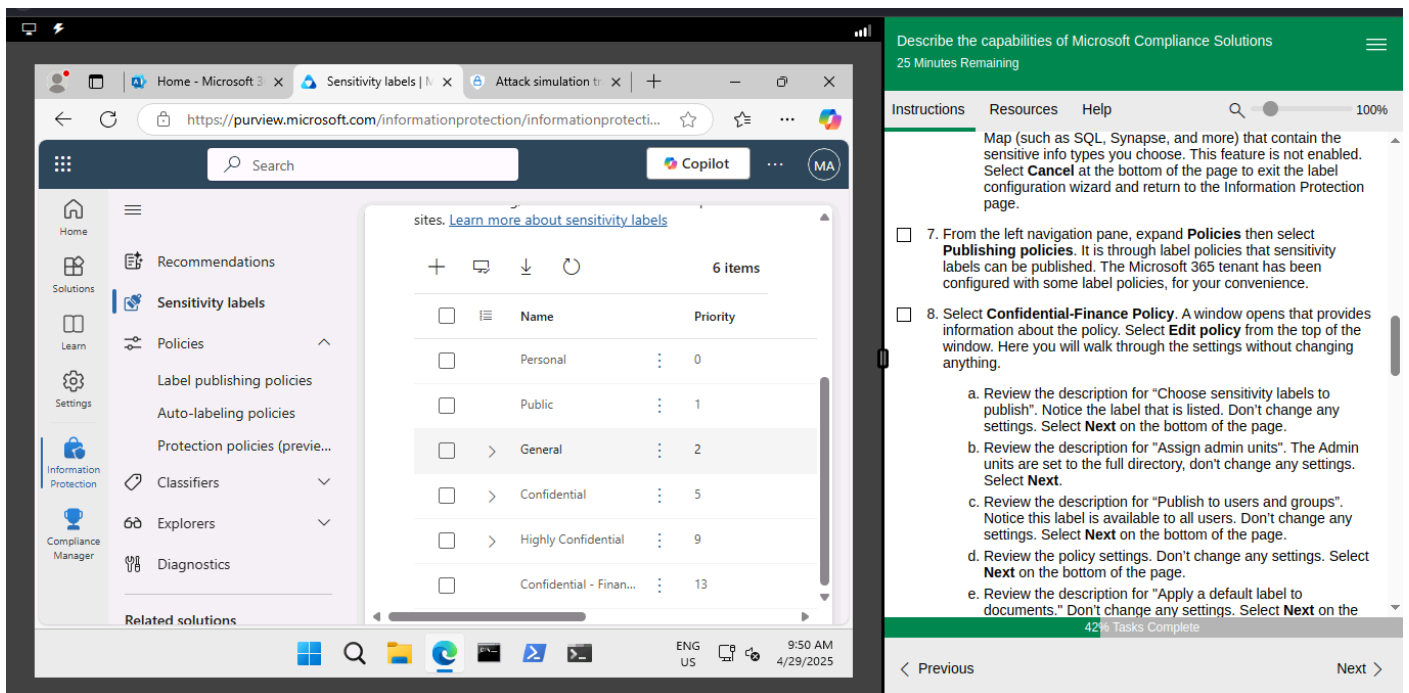
Instructions Resources Help

lab hoster (ALH).

- ☐ 2. From the left navigation pane of the Microsoft 365 admin center, select **Show all** then select **Compliance**. A new browser page opens to the welcome page of the Microsoft Purview portal.
- ☐ 3. In the left navigation panel, select **Solutions** then select **Information protection**. You are on the overview page. Scroll down to view the information available.
- ☐ 4. From the left navigation panel, select **Sensitivity labels**.
- ☐ 5. You will see a yellow banner indicating that your organization has not turned on the ability to process content in Office online files that have encrypted sensitivity labels applied and are stored in OneDrive and SharePoint. Select **Turn on now**.
- ☐ 6. Some labels have been preconfigured in your Microsoft 365 lab tenant, for your convenience. Select the label named **Confidential-Finance**. A window opens that provides information about this label. Note the settings for this label. Select **Edit label** if you don't see this option, select the ellipsis.
 - a. Configuration starts with providing basic details for the label. Don't change anything. Select **Next** at the bottom of the page.
 - b. Review the scope for this label. Don't change anything. Select **Next** at the bottom of the page.
 - c. This next screen is where you can choose protection settings for the labeled items. This label is configured to support

42% Tasks Complete

< Previous Next >



The screenshot shows the Microsoft Purview Sensitivity Labels page. The left navigation pane is the same as in the previous screenshot. The main content area shows a list of 6 items with columns for Name and Priority. The right sidebar contains instructions for the lab, starting with 'Map (such as SQL, Synapse, and more)' and listing steps 7 through 8.

Describe the capabilities of Microsoft Compliance Solutions
25 Minutes Remaining

Instructions Resources Help

Map (such as SQL, Synapse, and more) that contain the sensitive info types you choose. This feature is not enabled. Select **Cancel** at the bottom of the page to exit the label configuration wizard and return to the Information Protection page.

- ☐ 7. From the left navigation pane, expand **Policies** then select **Publishing policies**. It is through label policies that sensitivity labels can be published. The Microsoft 365 tenant has been configured with some label policies, for your convenience.
- ☐ 8. Select **Confidential-Finance Policy**. A window opens that provides information about the policy. Select **Edit policy** from the top of the window. Here you will walk through the settings without changing anything.
 - a. Review the description for "Choose sensitivity labels to publish". Notice the label that is listed. Don't change any settings. Select **Next** on the bottom of the page.
 - b. Review the description for "Assign admin units". The Admin units are set to the full directory, don't change any settings. Select **Next**.
 - c. Review the description for "Publish to users and groups". Notice this label is available to all users. Don't change any settings. Select **Next** on the bottom of the page.
 - d. Review the policy settings. Don't change any settings. Select **Next** on the bottom of the page.
 - e. Review the description for "Apply a default label to documents." Don't change any settings. Select **Next** on the

42% Tasks Complete

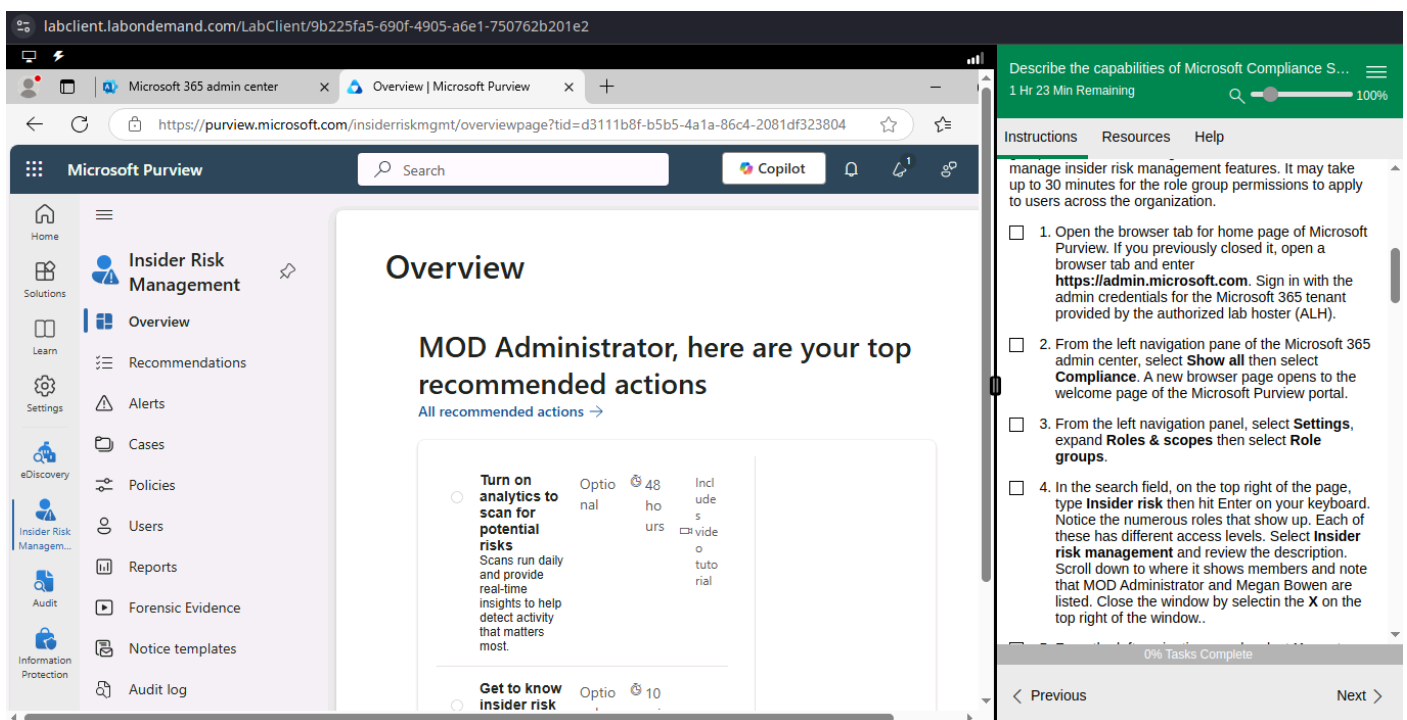
< Previous Next >

5. EXPLORE INSIDER RISK MANAGEMENT IN MICROSOFT PURVIEW

Insider Risk Management is a feature within Microsoft Purview designed to help organisations detect, investigate, and respond to potential internal threats by monitoring user behaviour across Microsoft 365 and beyond.

Its key capabilities include:

- Policy templates for common insider risks - pre-configured templates to help identify specific scenarios such as Data leaks, security policy violations, employee departure and sensitive data theft.
- User risk scoring- aggregates user behaviour signals to generate risk scores per user
- Case management and investigations- when suspicious behaviour is detected, the system automatically creates a case.
- Privacy- centric controls- investigations can be conducted with user identities anonymized until escalation is justified.



6. EXPLORE eDISCOVERY

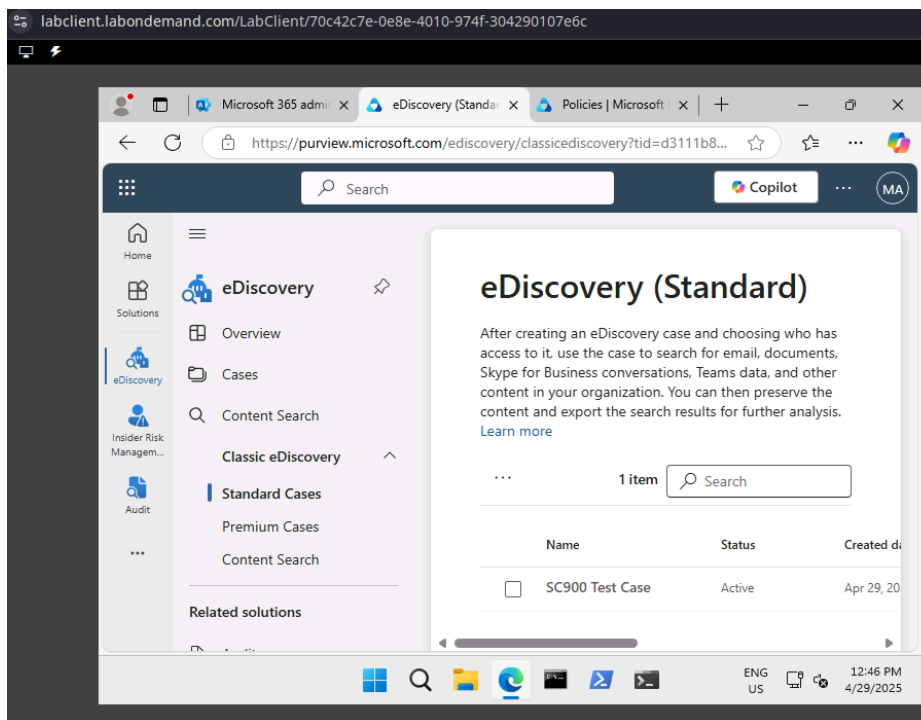
Electronic Discovery(eDiscovery) is a feature in Microsoft 365 services, Outlook/Exchange, SharePoint, OneDrive, or Teams, used to find, analyse, and export electronically stored information that might be needed for legal cases, investigations, or compliance reviews.

eDiscovery comes in three versions:

- Basic(Content search)- lets you search mailboxes, Teams chats, and files.
- Standard(eDiscovery)- includes everything in content search plus case management, legal holds, exporting results, audit trails of case activity.

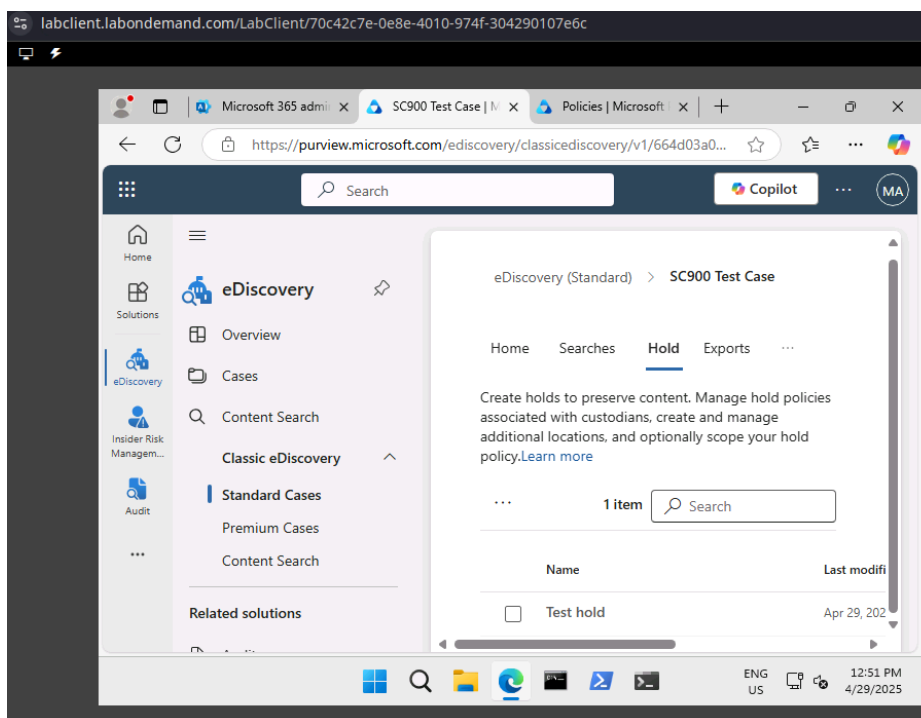
- Premium- adds upon the standard version with RBA, analytics and duplicate detection, review sets with tagging and redaction

Cases are created in the eDiscovery platform and used to search for content based on the set parameters of the case.



The screenshot shows the Microsoft Purview eDiscovery (Standard) interface. The left navigation pane includes options like Home, Solutions, eDiscovery, Insider Risk Management, and Audit. The main content area displays the 'eDiscovery (Standard)' page, which includes an overview section and a table with one item: 'SC900 Test Case'. The table has columns for Name, Status, and Created date. The status is 'Active' and the created date is 'Apr 29, 2025'.

On the right side, there is a sidebar with a green header 'Describe the capabilities of Microsoft Compliance...' and a progress bar showing '17 Minutes Remaining'. Below this, there are instructions and a list of tasks. Task 3 is highlighted, stating: 'Now that you've created an eDiscovery (Standard) case, you can begin to work with the case. In this task, you'll create an eDiscovery hold for the case for 76% Tasks Complete'.



The screenshot shows the Microsoft Purview eDiscovery (Standard) interface, specifically the 'SC900 Test Case' page. The left navigation pane is the same as in the previous screenshot. The main content area displays the 'SC900 Test Case' page, which includes a 'Hold' tab and a table with one item: 'Test hold'. The table has columns for Name and Last modified. The last modified date is 'Apr 29, 2025'.

On the right side, there is a sidebar with a green header 'Describe the capabilities of Microsoft Compliance...' and a progress bar showing '11 Minutes Remaining'. Below this, there are instructions and a list of tasks. Task 4 is highlighted, stating: 'With a hold in place, you'll create a search query. Once your search is complete, the eDiscovery supports actions, such as exporting and downloading the results for future investigation. Note: Searches associated with an eDiscovery (Standard) case are not listed on the Content search page in the Microsoft Purview portal. These searches are listed only on the Searches page of the associated eDiscovery (Standard) case.' Task 4 is 82% complete.

