

Name: Anne Musau

Program Details: Data Protection Specialist - C1 – 2025

Admission: adc-dp01-25032

Week 3 Lab Assignment: SC-900 Lab 3

Capabilities of Microsoft Compliance Solution.

1. Lab: Explore the Service Trust Portal
2. Lab: Explore the Microsoft Purview portal and Compliance Manager
3. Lab: Explore sensitivity labels in Microsoft Purview
4. Lab: Explore insider risk management in Microsoft Purview
5. Lab: Explore eDiscovery

1. Lab: Explore the Service Trust Portal

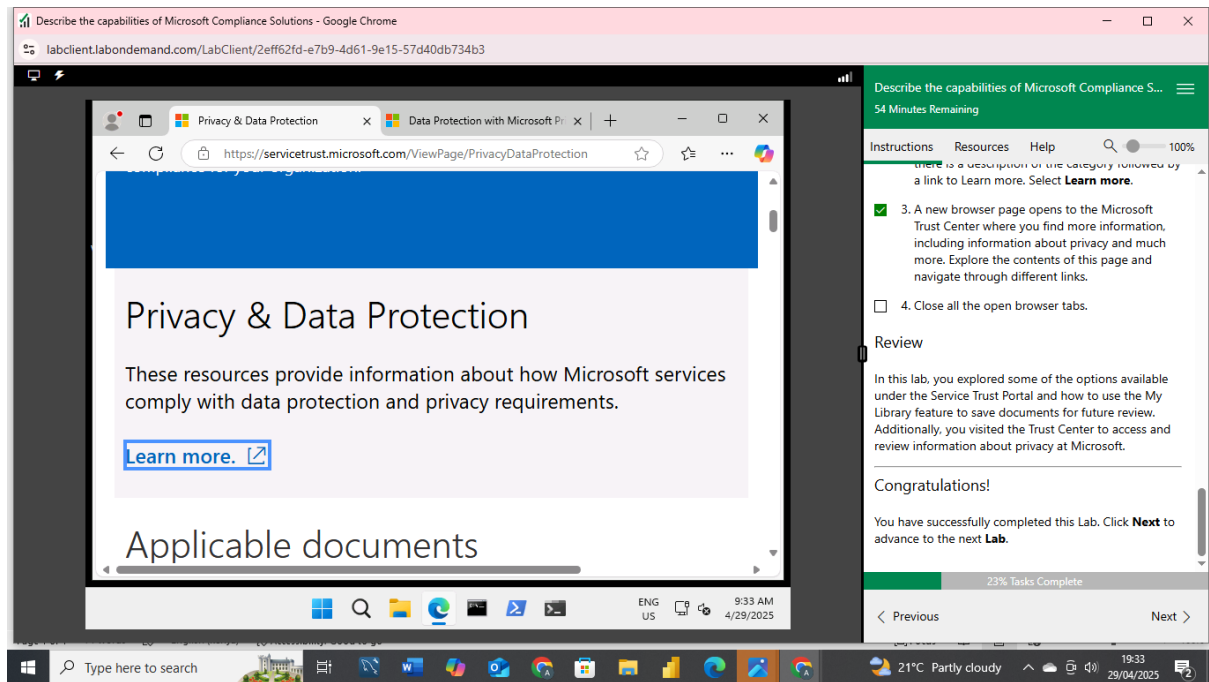
The screenshot displays a virtual lab environment. The main window shows a web browser with the URL <https://servicetrust.microsoft.com>. The page features the Microsoft logo and the title "Service Trust Portal". Below the title, it says "Learn how Microsoft cloud services protect your data, and how you can manage cloud data security and compliance for your organization." The page is decorated with icons representing security, privacy, and compliance.

On the right side of the browser window, there is a sidebar with the following content:

- Describe the capabilities of Microsoft Compliance S...** (with a menu icon)
- 1 Hour Remaining**
- Instructions Resources Help** (with a search icon and a 100% progress indicator)
- Lab: Explore the Service Trust Portal**
- This lab maps to the following Learn content:**
 - Learning Path: Describe the capabilities of Microsoft Privacy and Microsoft Purview
 - Module: Describe Microsoft's Service Trust portal and privacy capabilities
 - Unit: Explore the Service Trust Portal
- Lab scenario**

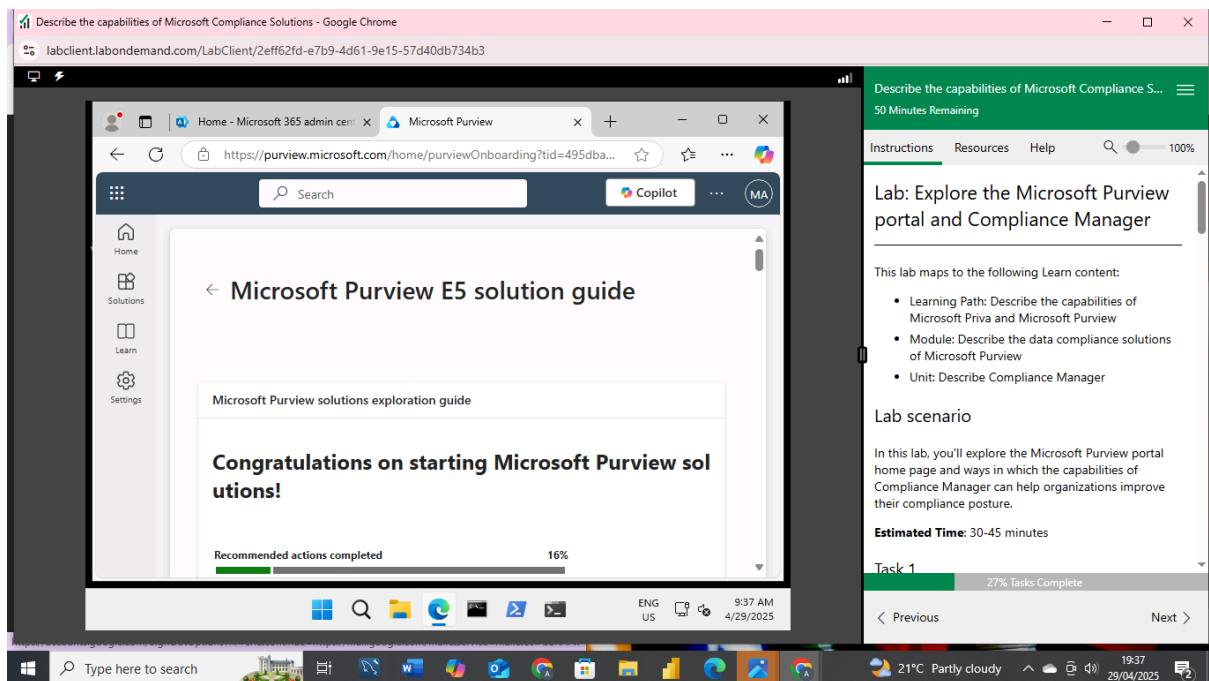
In this lab, you'll explore the features and content available from the Service Trust Portal. You'll also visit the Trust Center to view information about Privacy at Microsoft.
- Estimated Time:** 10-15 minutes
- Task 1**
- 20% Tasks Complete**
- < Previous** **Next >**

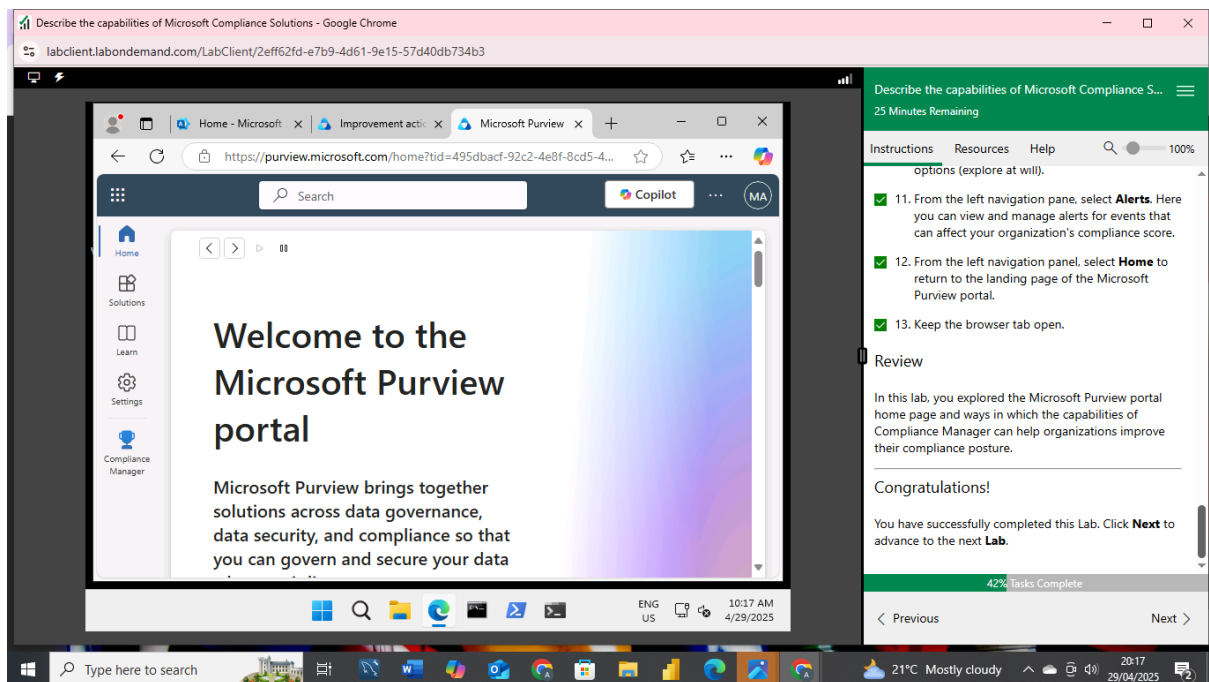
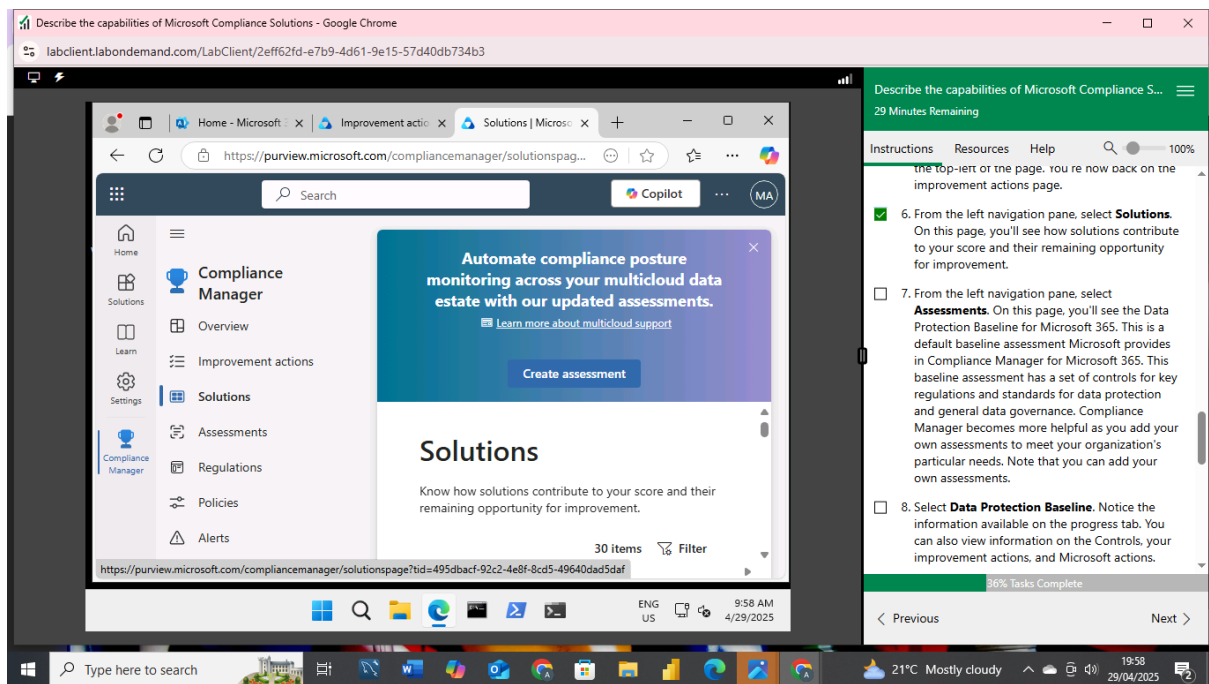
The bottom of the screen shows a Windows taskbar with various application icons, a search bar, and system tray information including the date (29/04/2025) and time (19:27).



In this lab, I learned how to navigate the Service Trust Portal and explored various compliance regulation documents, along with the different features available in the portal. I also visited the Trust Center to view information about Microsoft's privacy practices.

2. Lab: Explore the Microsoft Purview portal and Compliance Manager





In this lab, I explored the Microsoft Purview portal home page, which provides information on compliance posture status, available trials, recommendations, and more. I also examined the capabilities of the Compliance Manager, a tool that helps organizations improve their compliance posture. Compliance Manager helps assess and manage compliance for features such as Data Loss Prevention, Information Protection, Insider Risk Management, and Data Lifecycle Management. On the overview page on the compliance manager, I noted information on the compliance score, points achieved, and Microsoft managed points achieved.

3. Lab: Explore sensitivity labels in Microsoft Purview

The screenshot shows the Microsoft Purview Community landing page in a web browser. The page has a purple header with the text "Microsoft Purview Community" and "Dive into the Microsoft Purview Community". Below this, it says "Whether you're a seasoned expert or a curious newcomer, there's a place for you in the Microsoft Purview Community. Visit now to collaborate with and get answers from admins and Microsoft Purview team members." and a button "Go to Microsoft Purview Community".

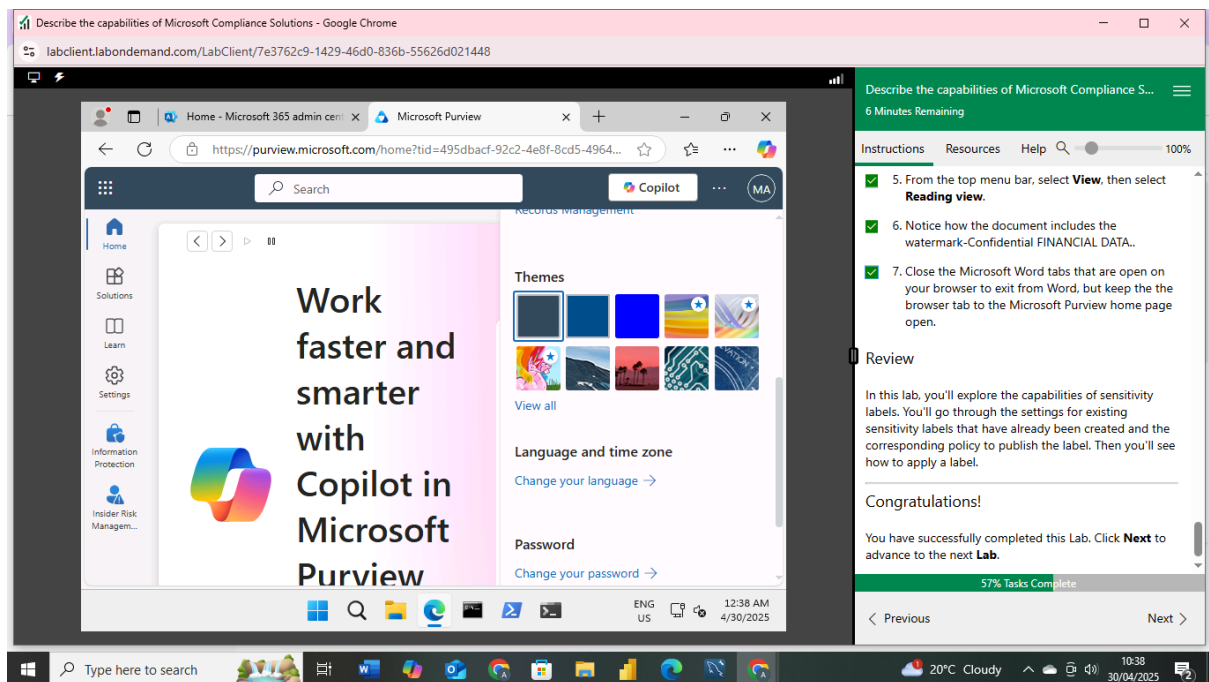
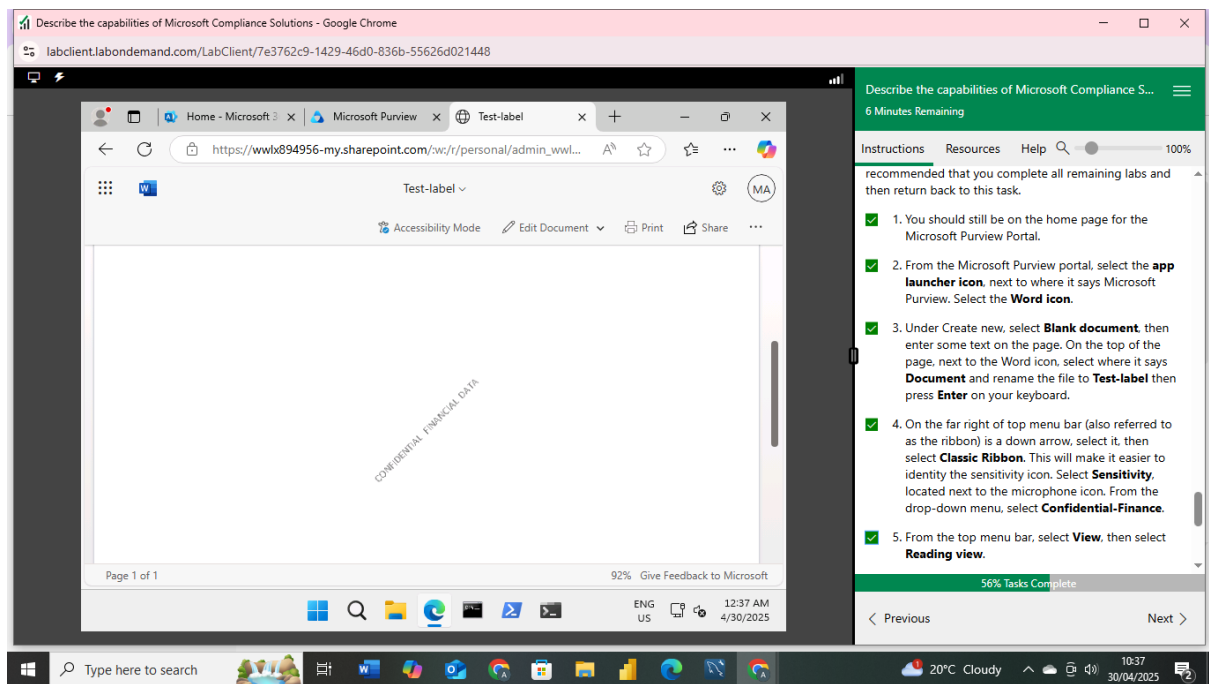
The sidebar on the right contains the following information:

- 21 Minutes Remaining
- Instructions Resources Help
- Lab: Explore sensitivity labels in Microsoft Purview
- This lab maps to the following Learn content:
 - Learning Path: Describe the capabilities of Microsoft Priva and Microsoft Purview
 - Module: Describe the data security solutions of Microsoft Purview
 - Unit: Describe sensitivity labels and policies in Microsoft Purview Information Protection
- Lab scenario
- In this lab, you'll explore the capabilities of sensitivity labels. You'll go through the settings for existing sensitivity labels that have been created and the corresponding policy to publish the label. Then you'll see how to apply a label and the impact of that label, from the perspective of a user.
- Estimated Time: 45 minutes
- 51% Tasks complete
- Previous Next

The screenshot shows the Microsoft Purview Auto-labeling policies page. The left navigation pane includes: Home, Solutions, Learn, Settings, Information Protection, and Insider Risk Management. The main content area shows a list of auto-labeling policies. A pop-up window titled "Protect PDFs with Auto-labeling" is displayed, showing a table with columns: Name, Locations, and Label a. The table has one row: "Off (1)".

The sidebar on the right contains the following information:

- 22 Minutes Remaining
- Instructions Resources Help
- Label policies page
- 9. From the left navigation panel, under Information protection, select Auto-labeling. Review the description. Note that you create auto-labeling policies to automatically apply sensitivity labels to email messages or OneDrive and SharePoint files that contain sensitive info. No auto-label policies have been preconfigured in our tenant. To create a new auto-label policy, select **Create auto-label policy**. Here you will walk through the steps to create a new policy.
- a. You start by choosing the information you want this label applied to. Note the available options. Select **Medical and health** then select one of the available templates. Select **Next**.
- b. You can name your auto-label policy or use the default name. Select **Next**.
- c. You can assign the admin units to which this policy applies. Leave the default set to full directory and select **Next**.
- d. Note the available locations where you want to apply the label. Leave the defaults.
- 50% Tasks complete
- Previous Next



In this lab, I explored sensitivity labels and label policies within Microsoft Purview Information Protection. I created an auto-labeling policy to automatically apply sensitivity labels to email messages, SharePoint files, and OneDrive content that contain sensitive information. I also created a sample test document to apply sensitivity labels manually. As part of the exercise, I applied a sensitivity label to a Microsoft Word document and observed the content marking specifically, a watermark generated by the label.

4. Lab: Explore insider risk management in Microsoft Purview

Describe the capabilities of Microsoft Compliance Solutions - Google Chrome

labclient.labondemand.com/LabClient/7e3762c9-1429-46d0-836b-55626d021448

Microsoft Purview

Work faster and smarter with Copilot in Microsoft Purview

Discover, analyze, and understand data faster with the power of AI.

Get started

Copilot

Alert summaries in Data Loss Prevention

Organize, prioritize, and speed up your alert handling process.

Learn more

Describe the capabilities of Microsoft Compliance Solutions - Google Chrome

1 Hr 22 Min Remaining

Instructions Resources Help

Lab: Explore insider risk management in Microsoft Purview

This lab maps to the following Learn content:

- Learning Path: Describe the capabilities of Microsoft Priva and Microsoft Purview
- Module: Describe the data security solutions of Microsoft Purview
- Unit: Describe insider risk management in Microsoft Purview

Lab scenario

In this lab, you'll walk through the process of setting up an insider risk policy, along with the basic prerequisites to configure and use insider risk management policies. Note: this lab will only provide visibility into what is required for setting up Insider risk management and options associated with creating a policy. This lab does not include a task to trigger the policy, as the number of 62% Tasks Complete

Previous Next

Describe the capabilities of Microsoft Compliance Solutions - Google Chrome

labclient.labondemand.com/LabClient/7e3762c9-1429-46d0-836b-55626d021448

Microsoft Purview

policy

Insider Risk Management

Overview Recommendations Alerts Cases Policies Users Reports Forensic Evidence

policies to ensure they're set up to detect the device activities you want to detect in your insider risk policies. Learn more about collection policies.

1 item

Policy name Status

SC900-Insider... Healthy

Describe the capabilities of Microsoft Compliance Solutions - Google Chrome

24 Minutes Remaining

Instructions Resources Help

Lab: Explore insider risk management in Microsoft Purview

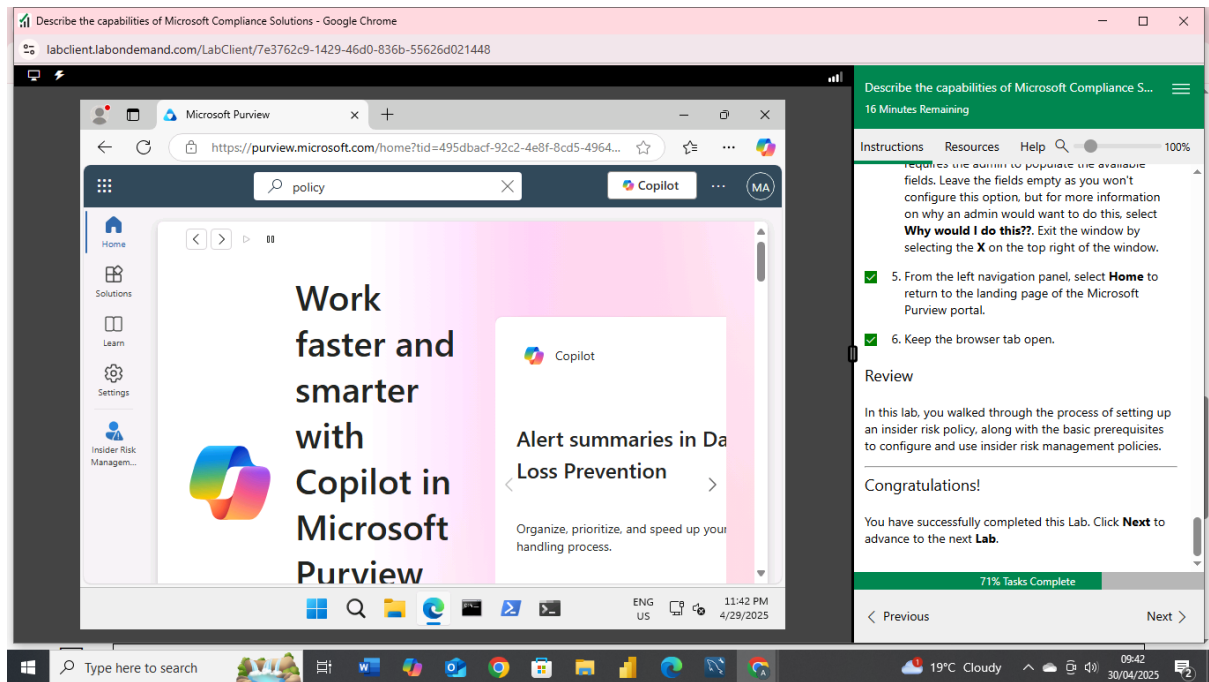
This lab maps to the following Learn content:

- Learning Path: Describe the capabilities of Microsoft Priva and Microsoft Purview
- Module: Describe the data security solutions of Microsoft Purview
- Unit: Describe insider risk management in Microsoft Purview

Lab scenario

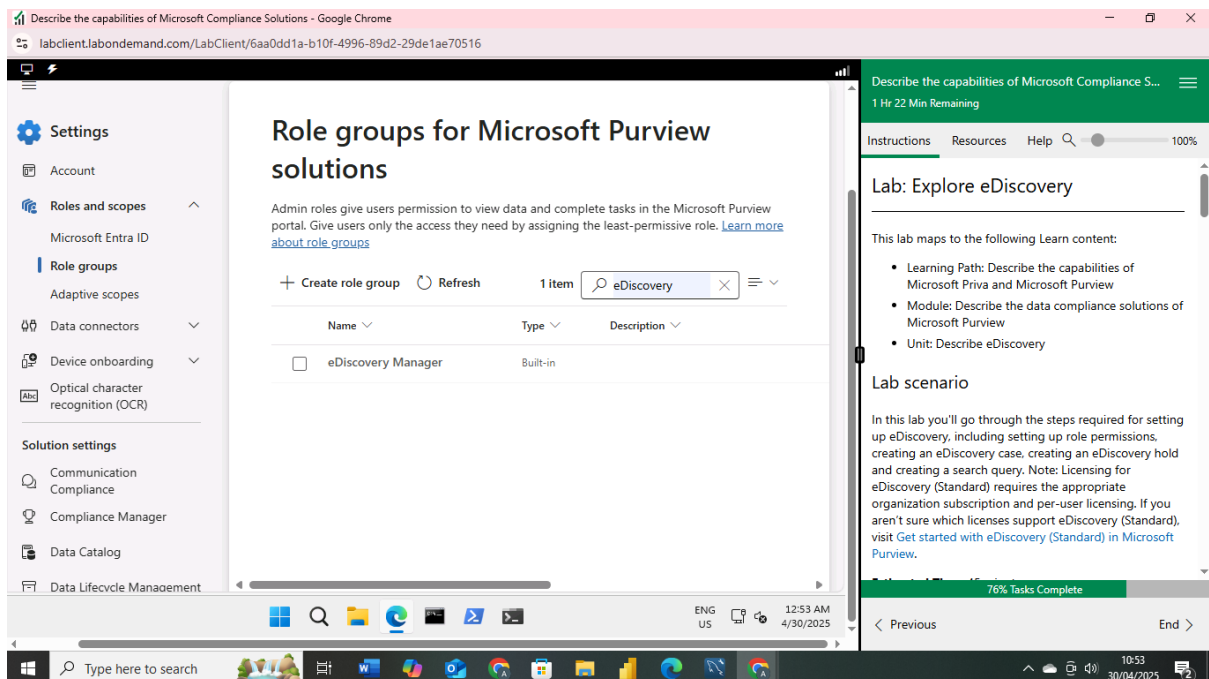
In this lab, you'll walk through the process of setting up an insider risk policy, along with the basic prerequisites to configure and use insider risk management policies. Note: this lab will only provide visibility into what is required for setting up Insider risk management and options associated with creating a policy. This lab does not include a task to trigger the policy, as the number of 62% Tasks Complete

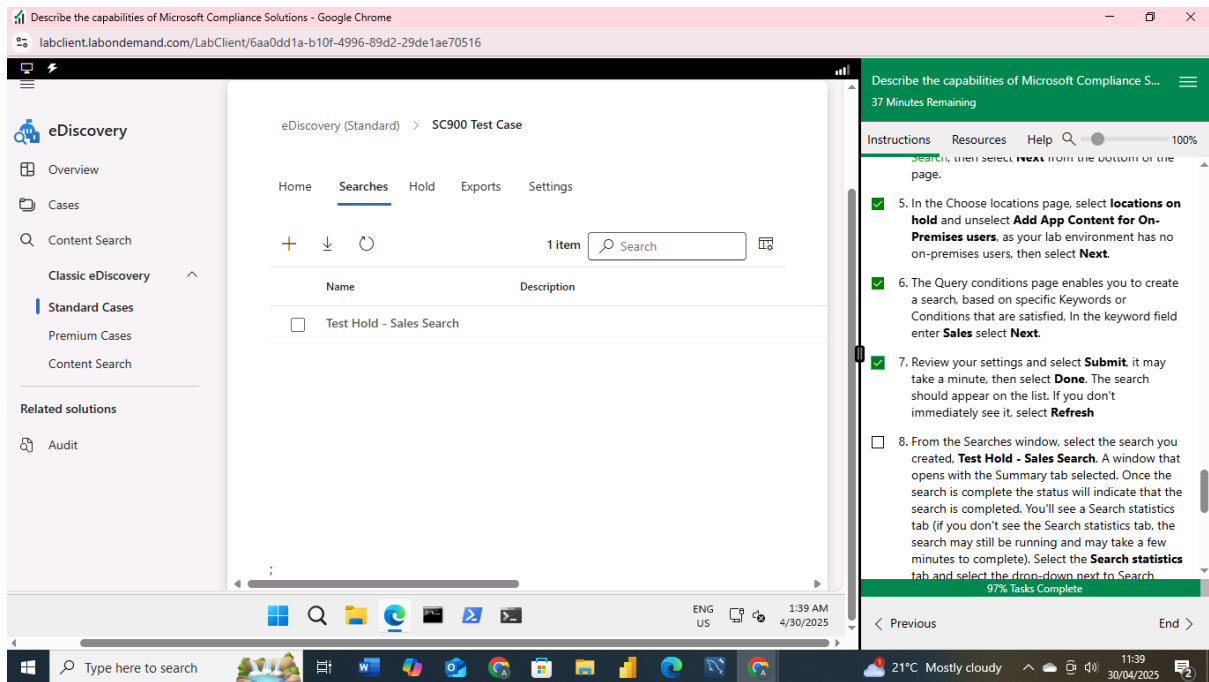
Previous Next



In this lab, I explored the necessary settings that must be configured before implementing an insider risk policy. I then proceeded to create an insider risk policy to help identify and manage potential internal threats within the organization.

5. Lab: Explore eDiscovery





In the eDiscovery lab, I created an eDiscovery case and assigned an Administrator to grant access to the case. I used the case to search for content across email, documents, Teams data, and other sources. Additionally, I placed a hold on the case to preserve relevant content. With the hold in place, I created and executed a search query within the case.