**NAME: BINYANYA DEBORAH NYATICHI**

**CS NO: ADC-CSS02-25051**.

**DESCRIPTION: Week 4 Assignment 7**

**ASSIGNMENT: Lab Describe the capabilities of Microsoft Compliance Solutions**

**DATE: 02/05/2025**

# INTRODUCTION

This week, I will be embarking on a series of labs designed to build a practical understanding of Microsoft's comprehensive suite of compliance solutions. My journey will begin with the essential step of setting up a Microsoft 365 tenant, providing the foundational environment for exploring these capabilities. From there, I will delve into the **Service Trust Portal** to understand Microsoft's commitment to security, compliance, and privacy. The core of my exploration will then focus on the **Microsoft Purview portal** and its **Compliance Manager**, where I will learn to navigate and utilize tools for data governance and risk management. Finally, I will gain hands-on experience with specific Purview features, including the creation and application of **sensitivity labels**, the identification and mitigation of **insider risks**, and the processes involved in **eDiscovery**. Through these labs, I aim to develop a tangible understanding of how organizations can leverage Microsoft's tools to meet their compliance obligations, protect sensitive data, and manage potential risks effectively.

# LAB: SETUP OF THE MICROSOFT 365 TENANT

## Lab scenario

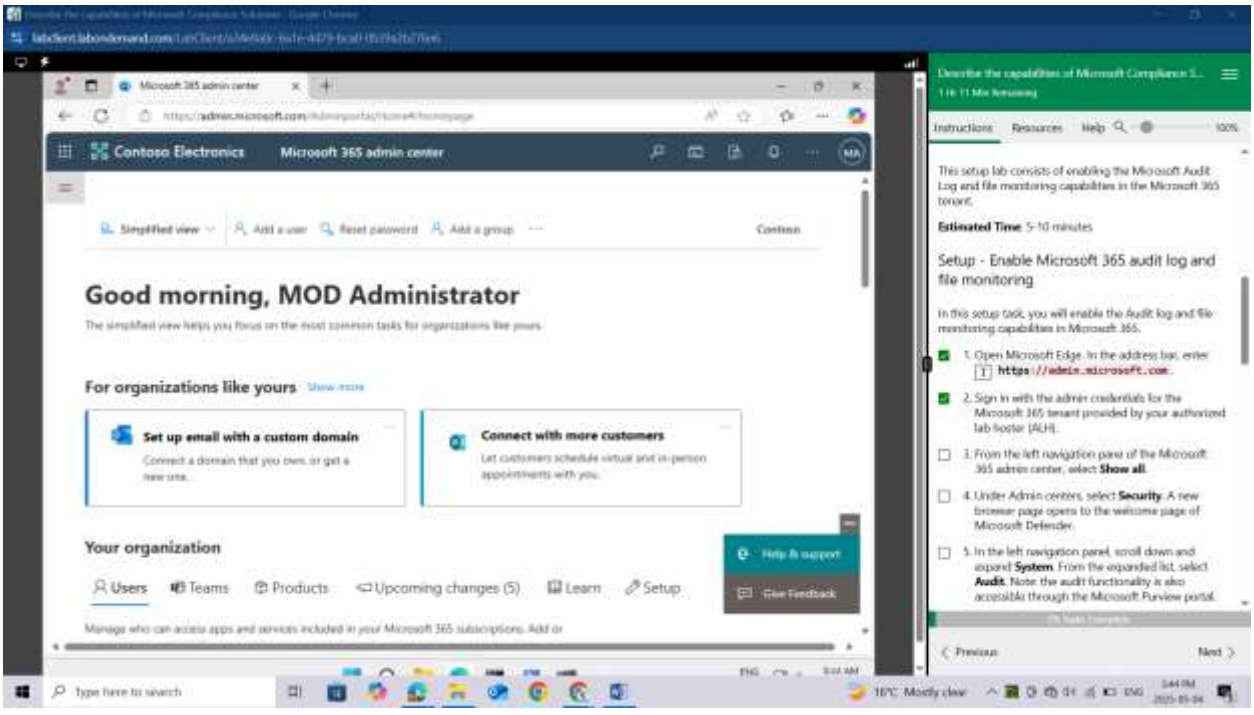
This setup lab consists of enabling the Microsoft Audit Log and file monitoring capabilities in the Microsoft 365 tenant.

Setup - Enable Microsoft 365 audit log and file monitoring

In this setup task, you will enable the Audit log and file monitoring capabilities in Microsoft 365.

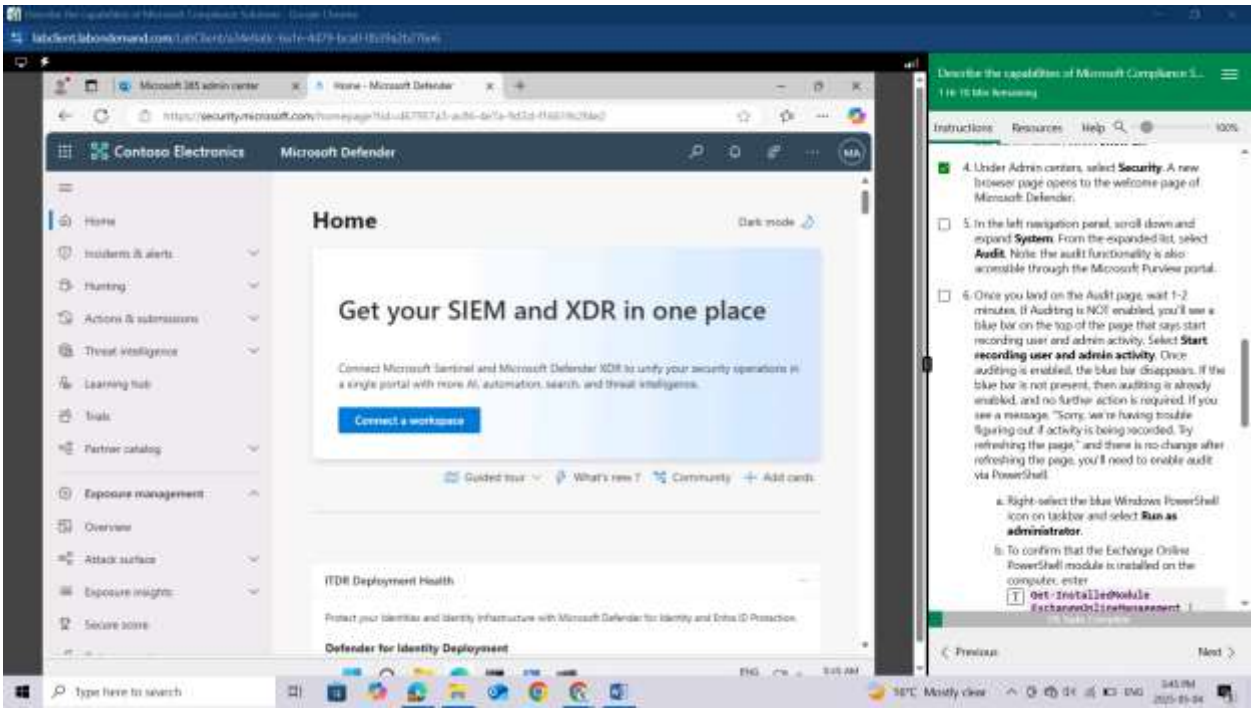
Open Microsoft Edge. In the address bar, enter https://admin.microsoft.com.

Sign in with the admin credentials for the Microsoft 365 tenant provided by your authorized lab hoster (ALH).



From the left navigation pane of the Microsoft 365 admin center, select **Show all.**

Under Admin centers, select **Security**. A new browser page opens to the welcome page of Microsoft Defender.




In the left navigation panel, scroll down and expand **System**. From the expanded list, select **Audit**. Note: the audit functionality is also accessible through the Microsoft Purview portal.

Once you land on the Audit page, wait 1-2 minutes. If Auditing is NOT enabled, you'll see a blue bar on the top of the page that says start recording user and admin activity. Select Start recording user and admin activity. Once auditing is enabled, the blue bar disappears. If the blue bar is not present, then auditing is already enabled, and no further action is required. If you see a message, "Sorry, we're having trouble figuring out if activity is being recorded. Try refreshing the page," and there is no change after refreshing the page, you'll need to enable audit via PowerShell.

Right-select the blue Windows PowerShell icon on taskbar and select Run as administrator.

To confirm that the Exchange Online PowerShell module is installed on the computer, enter Get-InstalledModule ExchangeOnlineManagement | Format-List Name,Version,InstalledLocation. You'll see the name, version and installed location of Exchange OnlineManagement.

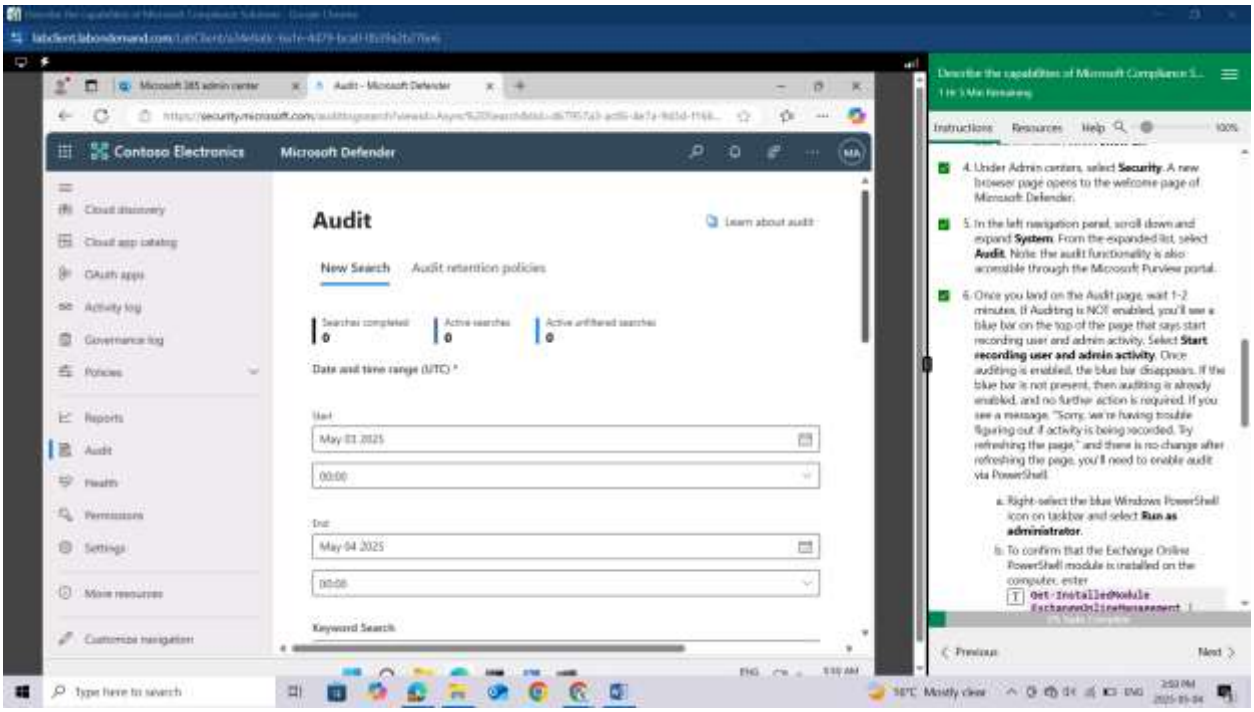
Now load the module, by entering Import-Module ExchangeOnlineManagement.

To connect, enter Connect-ExchangeOnline -UserPrincipalName admin@WWLxZZZZZZ.onmicrosoft.com. For the UPN, enter the administrator username found in the resources tab of your lab.

You'll be prompted to sign in. Enter the administrative username and password found in the resources tab of your lab.

To turn on Auditing, enter Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true. A message is displayed saying that it might take up to 60 minutes for the change to take effect.

Although it may take up to 60 minutes to take effect, you can verify the command was received by entering Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled. If audit is enabled, the property UnifiedAuditLogIngestionEnabled will show a value of true.

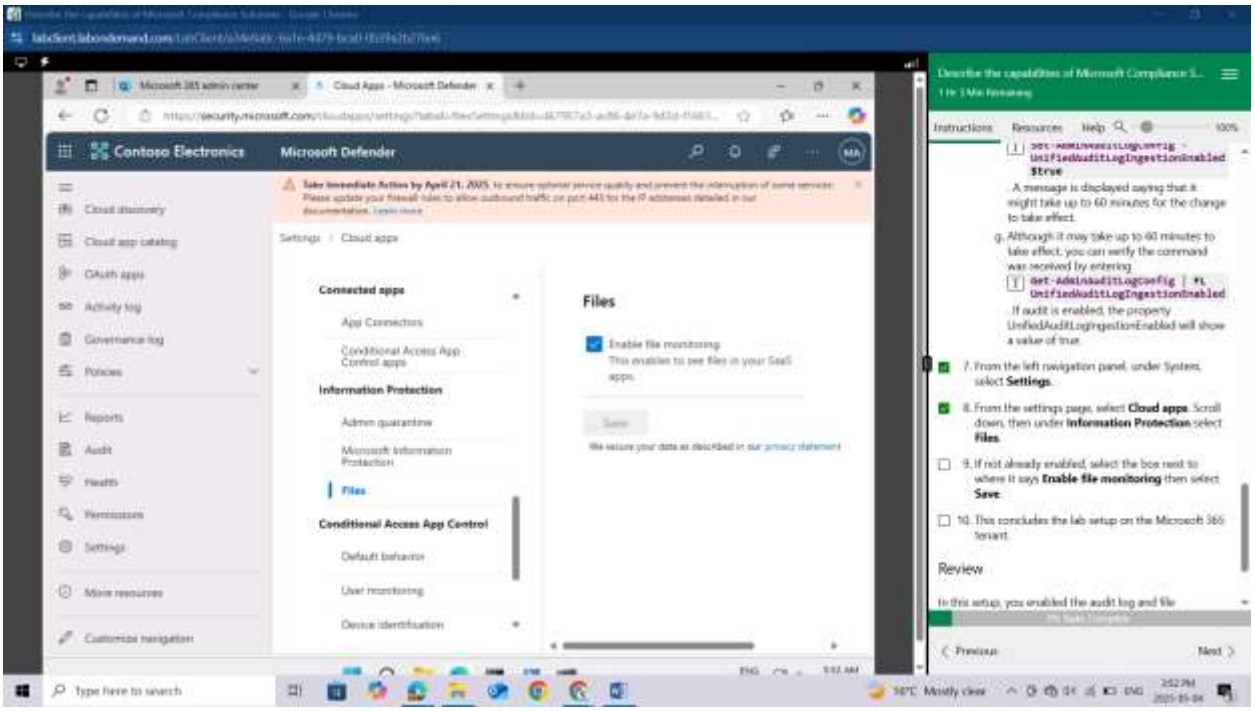



From the left navigation panel, under System, select Settings.

From the settings page, select Cloud apps. Scroll down, then under Information Protection select Files.

If not already enabled, select the box next to where it says Enable file monitoring then select Save.

This concludes the lab setup on the Microsoft 365 tenant.




# LAB: EXPLORE THE SERVICE TRUST PORTAL

This lab maps to the following Learn content:

Learning Path: Describe the capabilities of Microsoft Priva and Microsoft Purview

Module: Describe Microsoft's Service Trust portal and privacy capabilities

Unit: Explore the Service Trust Portal

## Lab scenario

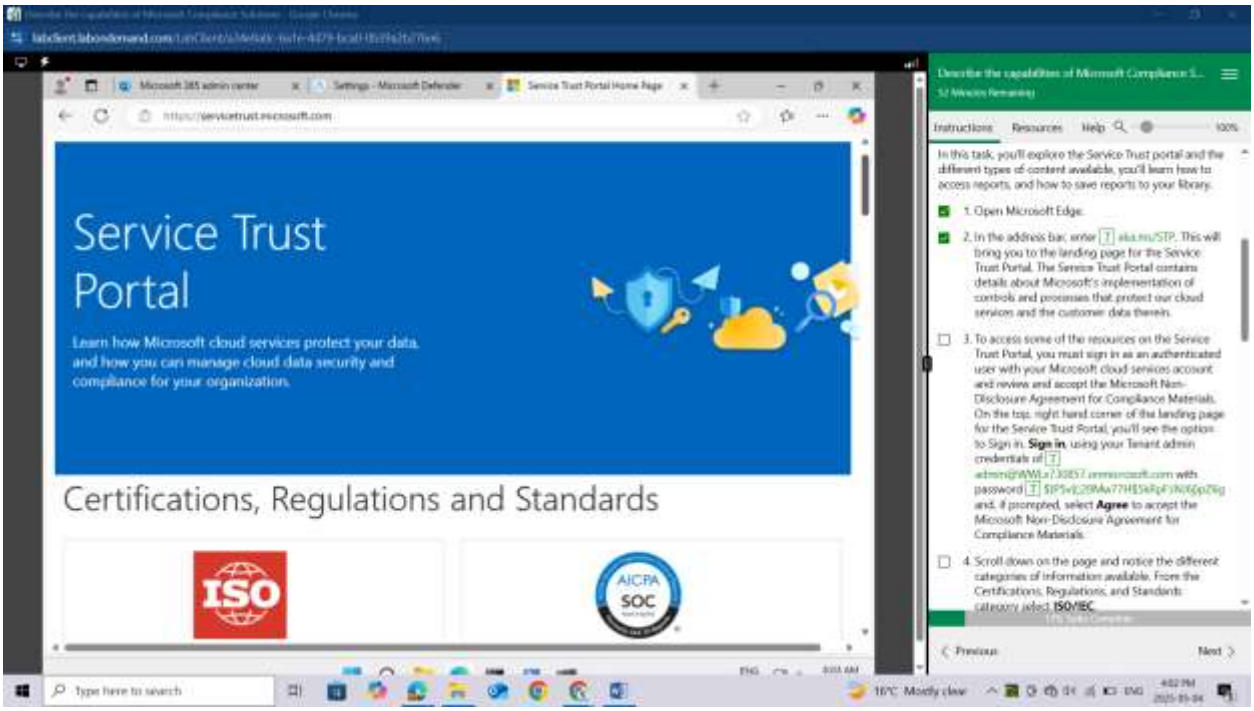
In this lab, you'll explore the features and content available from the Service Trust Portal. You'll also visit the Trust Center to view information about Privacy at Microsoft.

## 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.

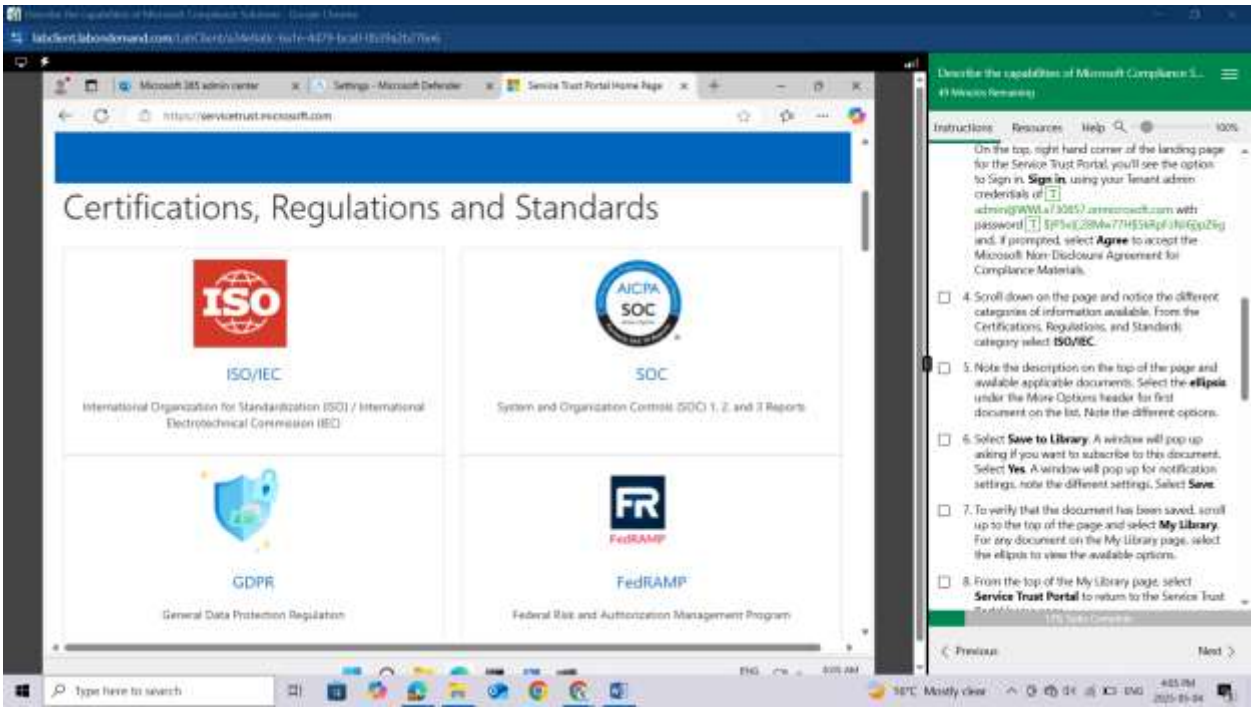
Open Microsoft Edge.

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.

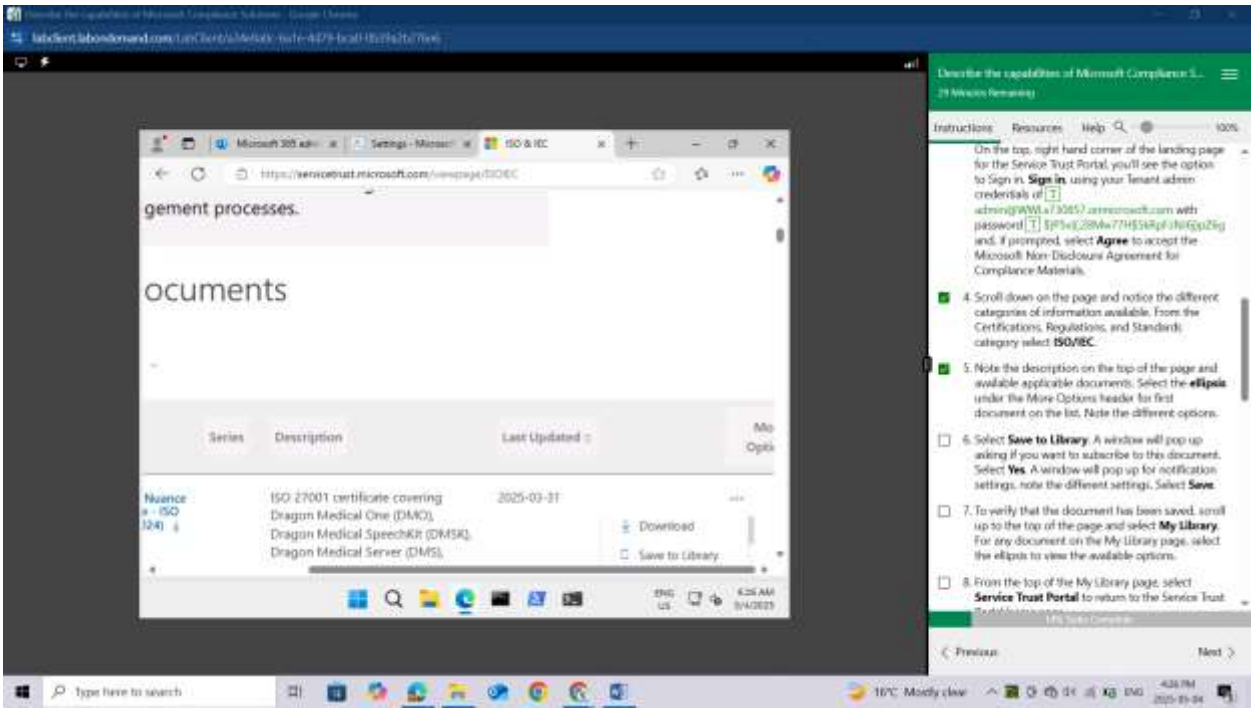



To access some of the resources on the Service Trust Portal, you must sign in as an authenticated user with your Microsoft cloud services account and review and accept the Microsoft Non-Disclosure Agreement for Compliance Materials. On the top, right hand corner of the landing page for the Service Trust Portal, you'll see the option to Sign in. Sign in, using your Tenant admin credentials of admin@WWLx730857.onmicrosoft.com with password $)P5v{(;28Mw77H$5kRpF:iNJ6j)pZ6g and, if prompted, select Agree to accept the Microsoft Non-Disclosure Agreement for Compliance Materials.

Scroll down on the page and notice the different categories of information available. From the Certifications, Regulations, and Standards category select ISO/IEC.

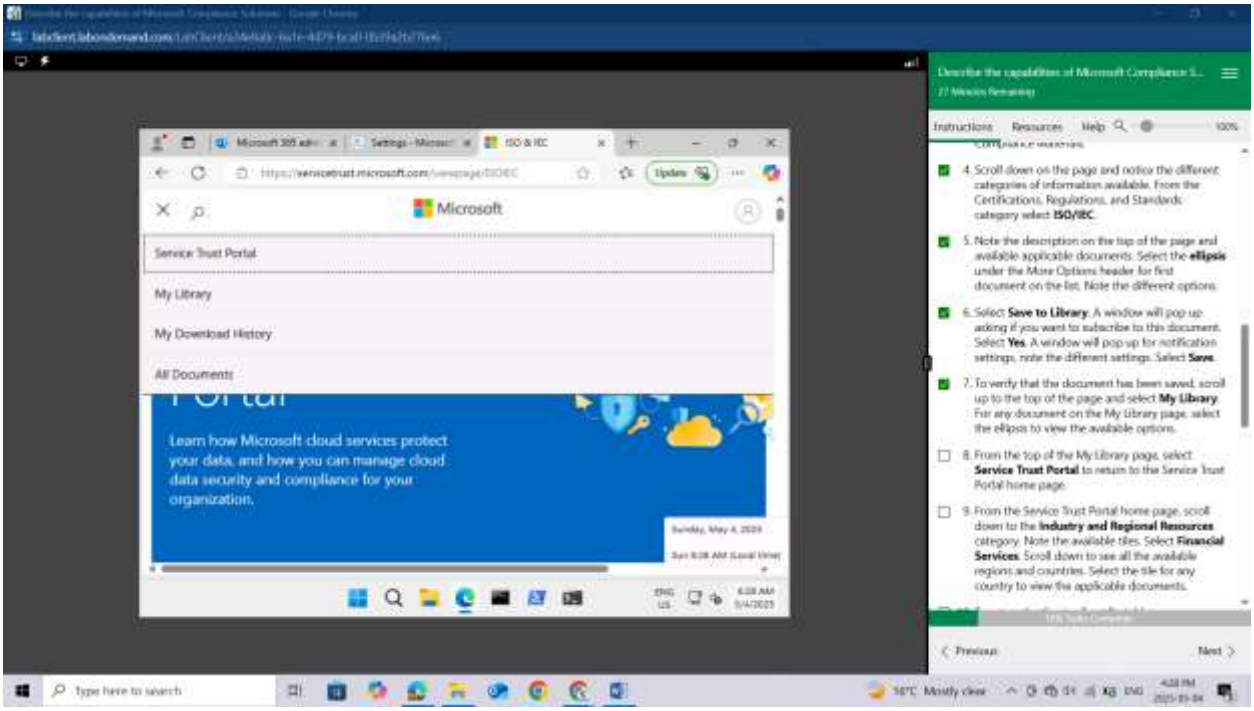



Note the description on the top of the page and available applicable documents. Select the ellipsis under the More Options header for first document on the list. Note the different options.

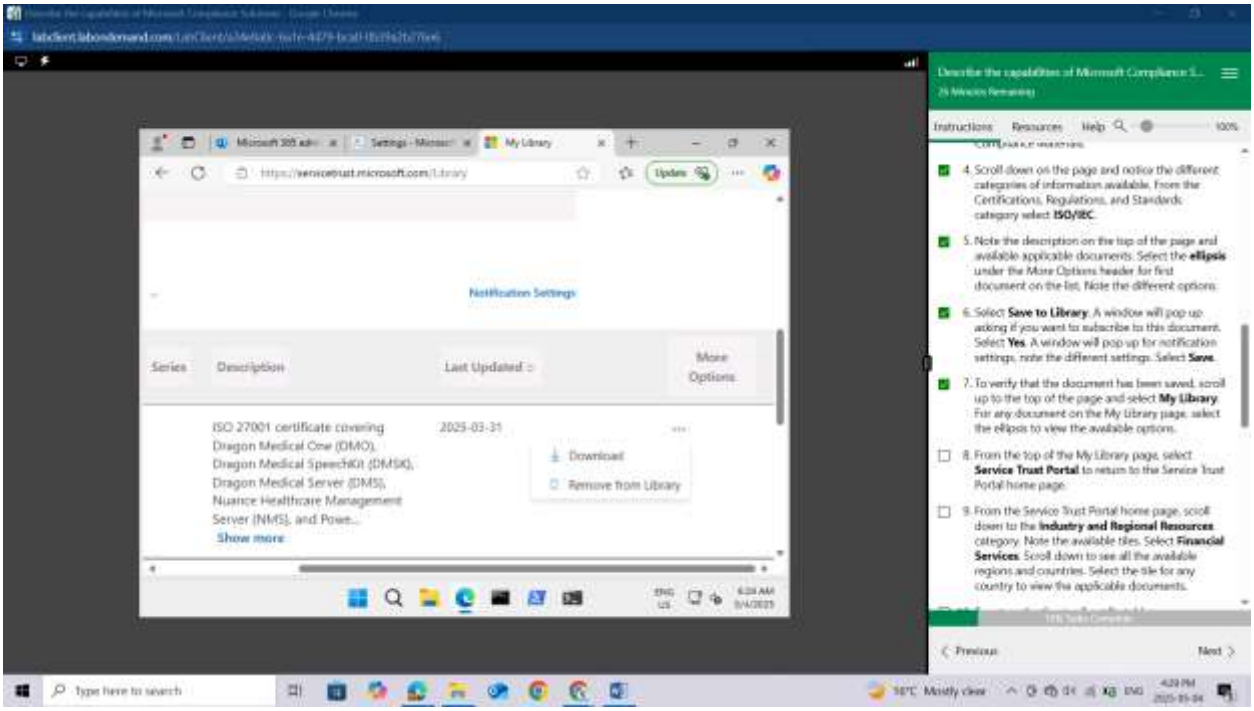



Select **Save to Library**. A window will pop up asking if you want to subscribe to this document. Select Yes. A window will pop up for notification settings, note the different settings. Select Save.

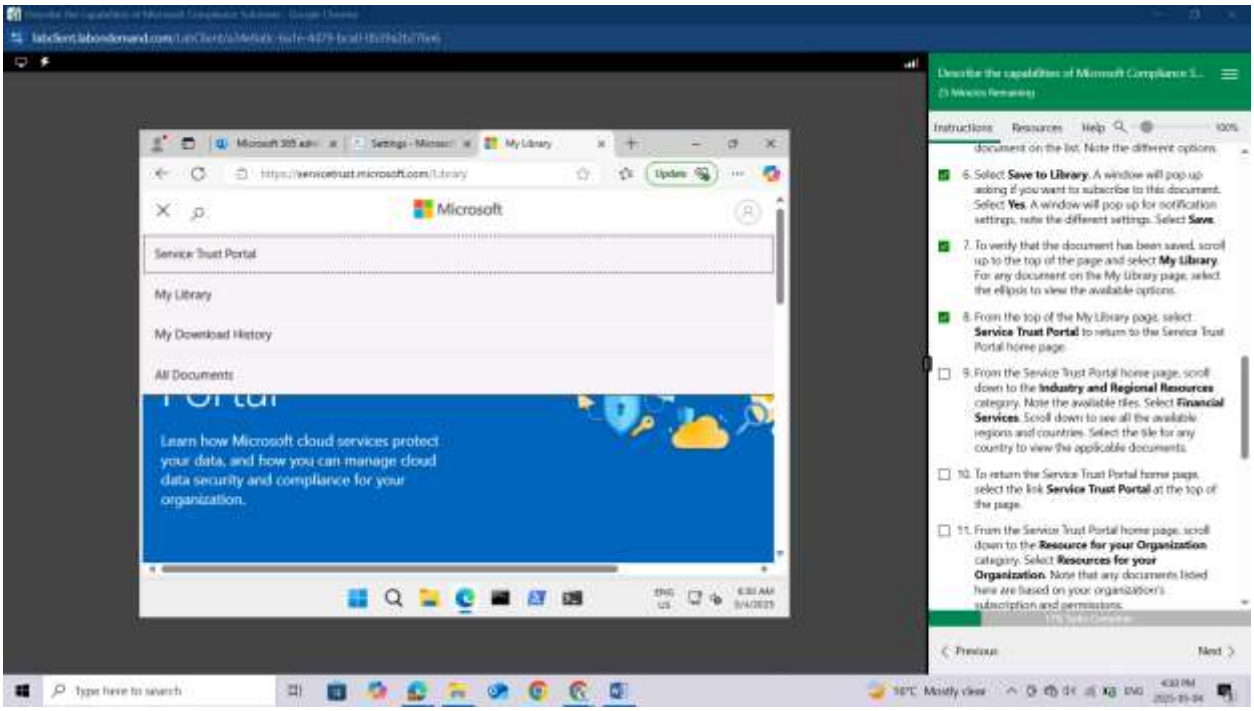
To verify that the document has been saved, scroll up to the top of the page and select **My Library**.



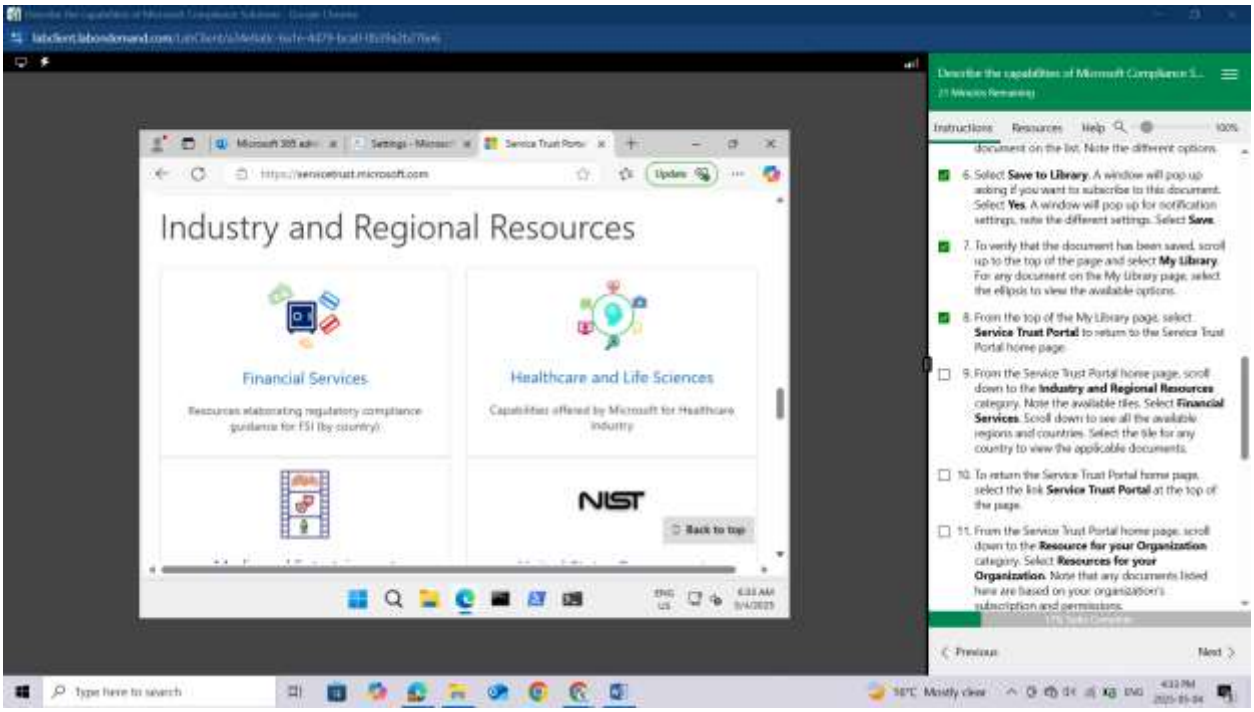

For any document on the **My Library** page, select the **ellipsis** to view the available options.



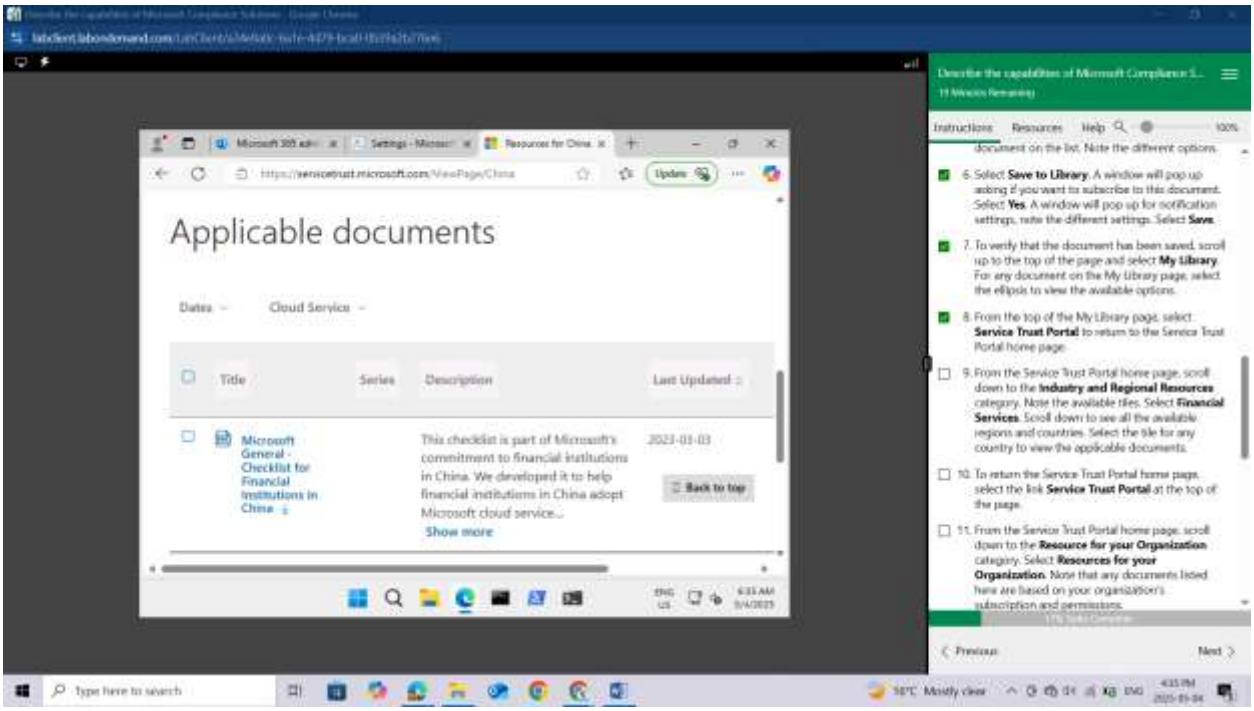

From the top of the My Library page, select **Service Trust Portal** to return to the Service Trust Portal home page.




From the Service Trust Portal home page, scroll down to the Industry and Regional Resources category. Note the available tiles.

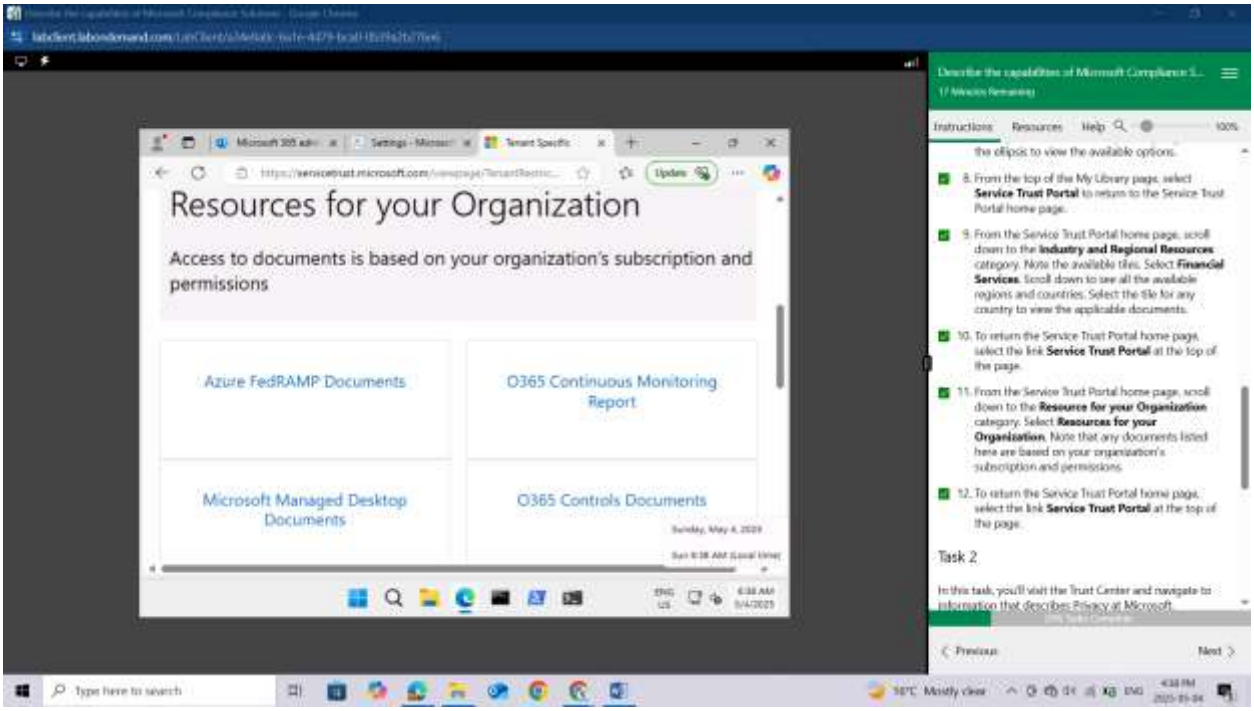



Select Financial Services. Scroll down to see all the available regions and countries. Select the tile for any country to view the applicable documents.




To return the Service Trust Portal home page, select the link Service Trust Portal at the top of the page.

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.

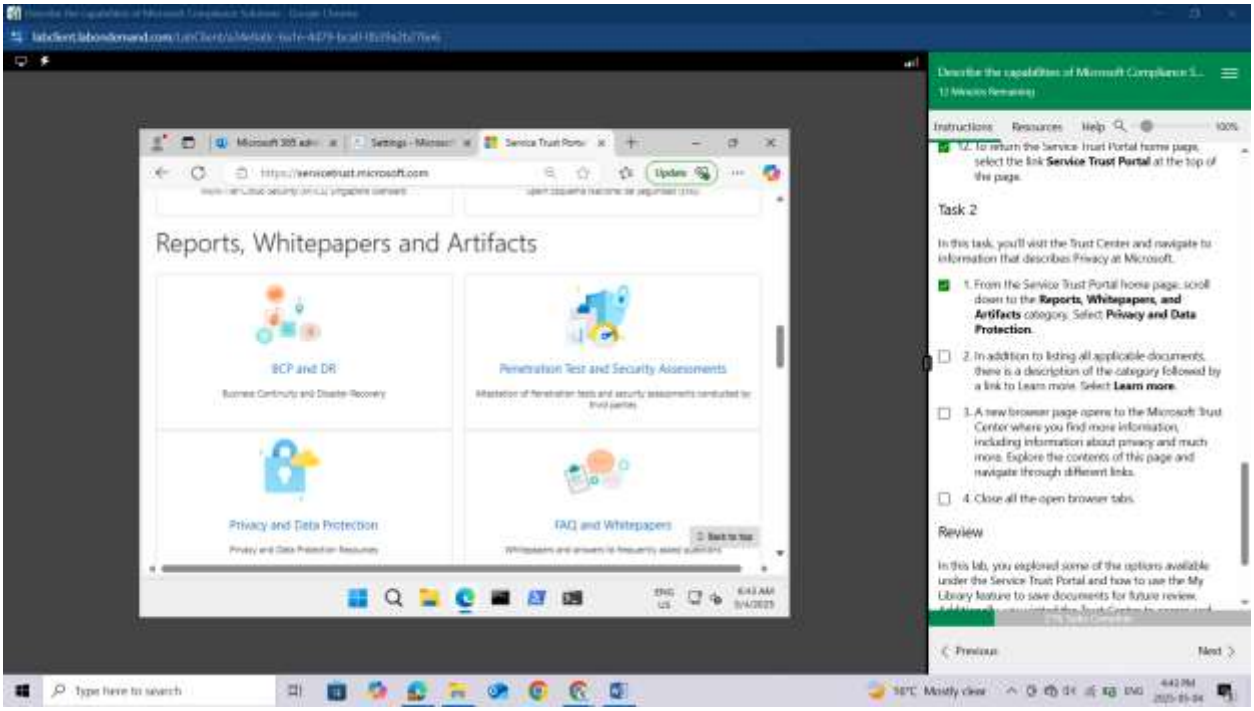



To return the Service Trust Portal home page, select the link Service Trust Portal at the top of the page.

## Task 2

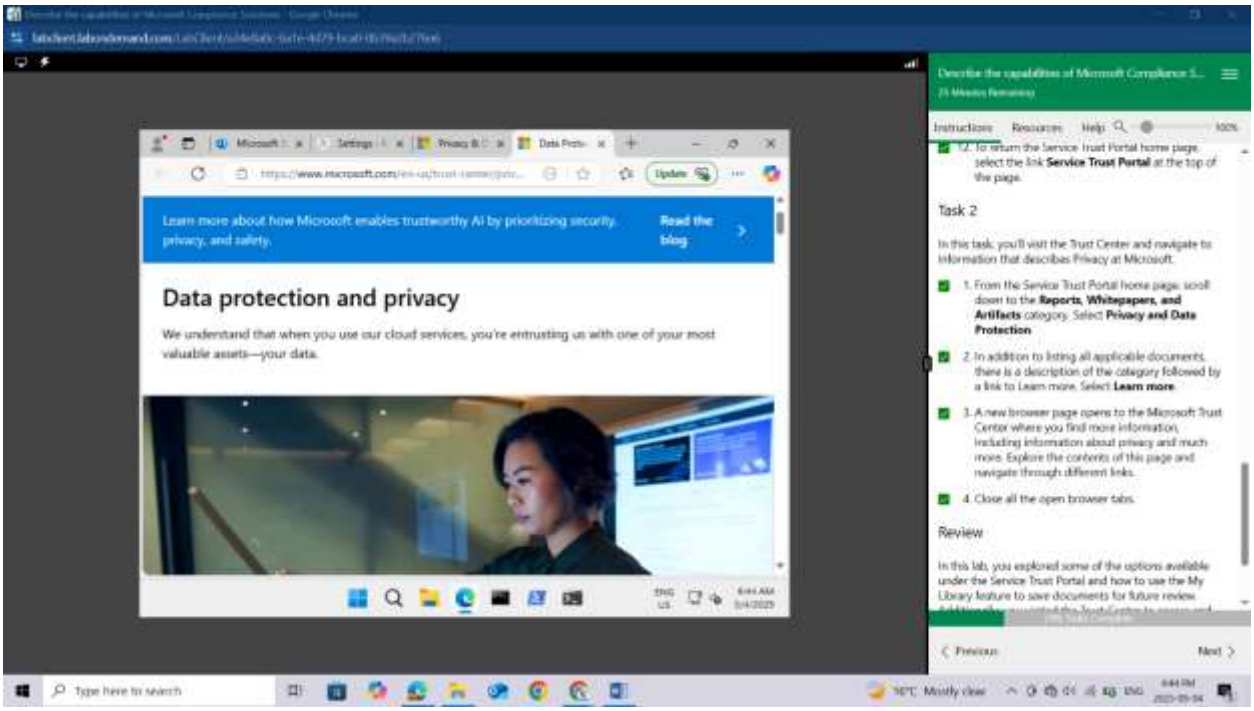
In this task, you'll visit the Trust Center and navigate to information that describes Privacy at Microsoft.

From the Service Trust Portal home page, scroll down to the Reports, Whitepapers, and Artifacts category. Select **Privacy and Data Protection.**




In addition to listing all applicable documents, there is a description of the category followed by a link to Learn more. Select Learn more.

A new browser page opens to the Microsoft Trust Center where you find more information, including information about privacy and much more. Explore the contents of this page and navigate through different links.




Close all the open browser tabs.

# LAB: EXPLORE THE MICROSOFT PURVIEW PORTAL AND COMPLIANCE MANAGER

This lab maps to the following Learn content:

Learning Path: Describe the capabilities of Microsoft Priva and Microsoft Purview

Module: Describe the data compliance solutions of Microsoft Purview

Unit: Describe Compliance Manager

## Lab scenario

In this lab, you'll explore the Microsoft Purview portal home page and ways in which the capabilities of Compliance Manager can help organizations improve their compliance posture.

## Task 1

Explore the Microsoft Purview portal home page.

Open Microsoft Edge. In the address bar, enter admin.microsoft.com.

Sign in with your admin credentials.

In the Sign in window, enter admin@WWLx730857.onmicrosoft.com then select **Next**.

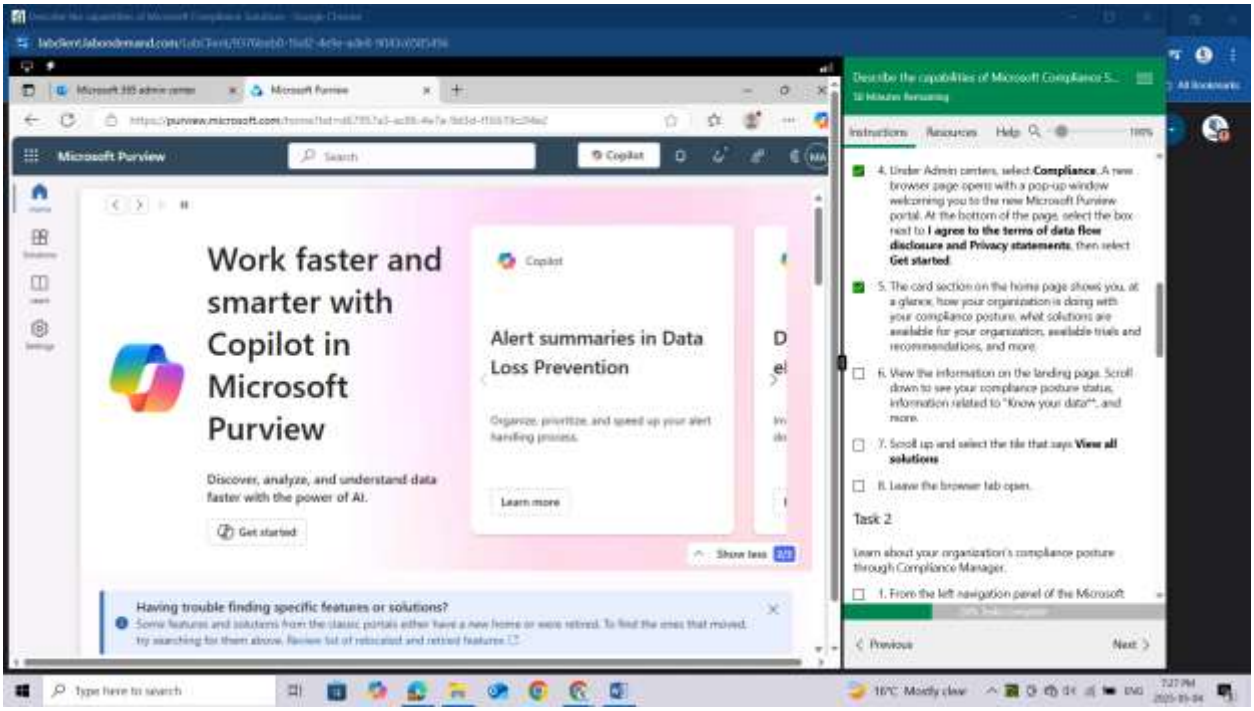
Enter the admin password that should be provided by your lab hosting provider. Select **Sign in.**

Depending on your lab hoster and if this is the first time you are logging in to the tenant, you may be prompted to complete the MFA registration process. If so, follow the prompts on the screen to setup MFA.

Once you're signed-in, you're taken to the Microsoft 365 admin center page.

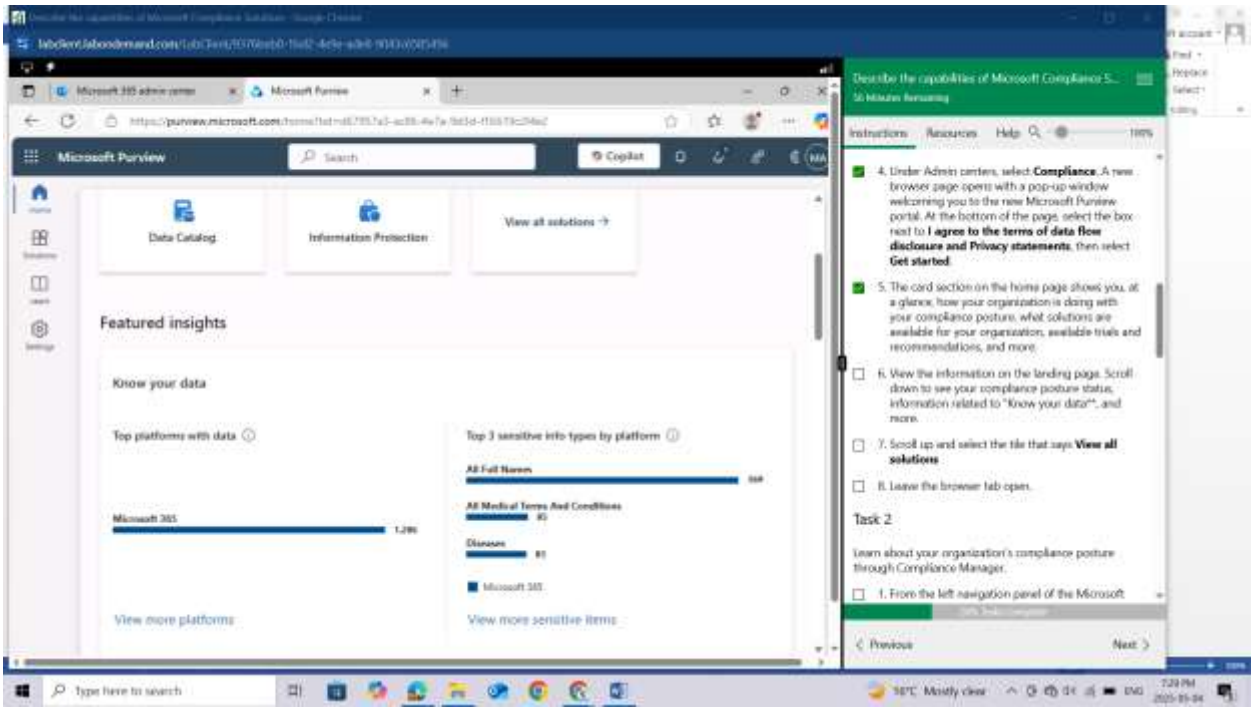
From the left navigation pane of the Microsoft 365 admin center, select **Show all**.

Under Admin centers, select Compliance. A new browser page opens with a pop-up window welcoming you to the new Microsoft Purview portal. At the bottom of the page, select the box next to I agree to the terms of data flow disclosure and Privacy statements, then select **Get started**.



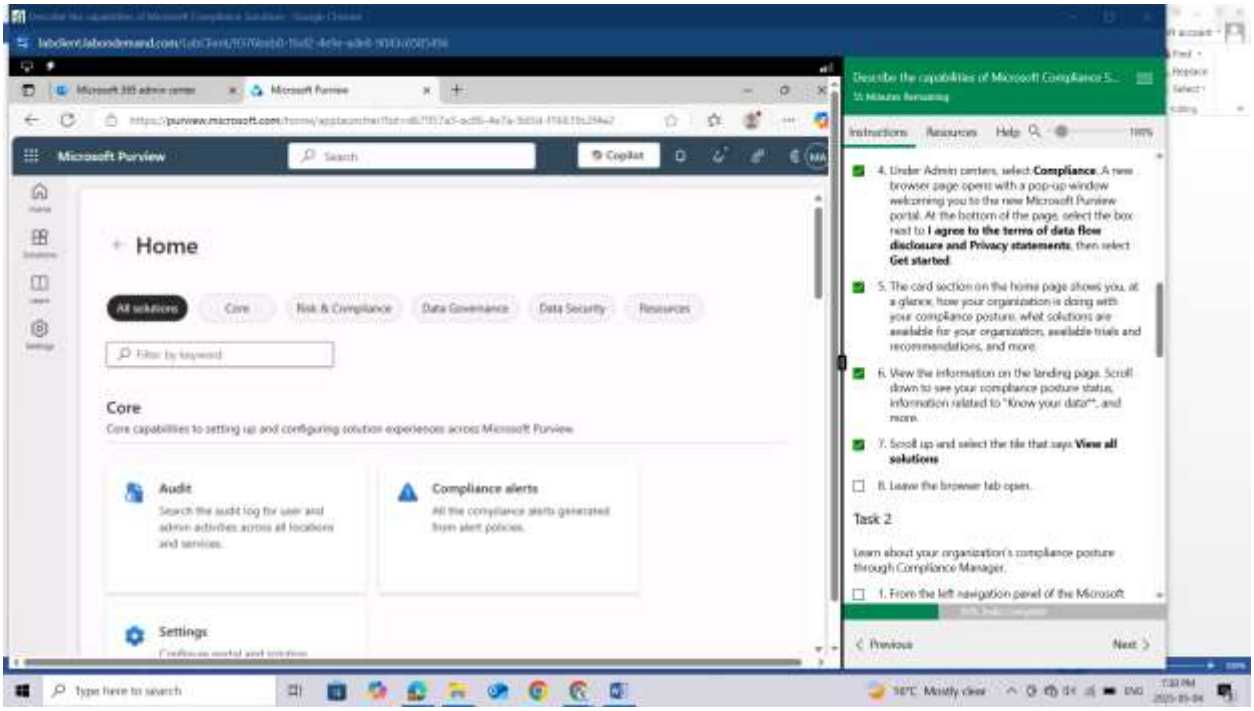

The card section on the home page shows you, at a glance, how your organization is doing with your compliance posture, what solutions are available for your organization, available trials and recommendations, and more.

View the information on the landing page. Scroll down to see your compliance posture status, information related to "**Know your data**,** and more.




Scroll up and select the tile that says **View all solutions**

Leave the browser tab open.

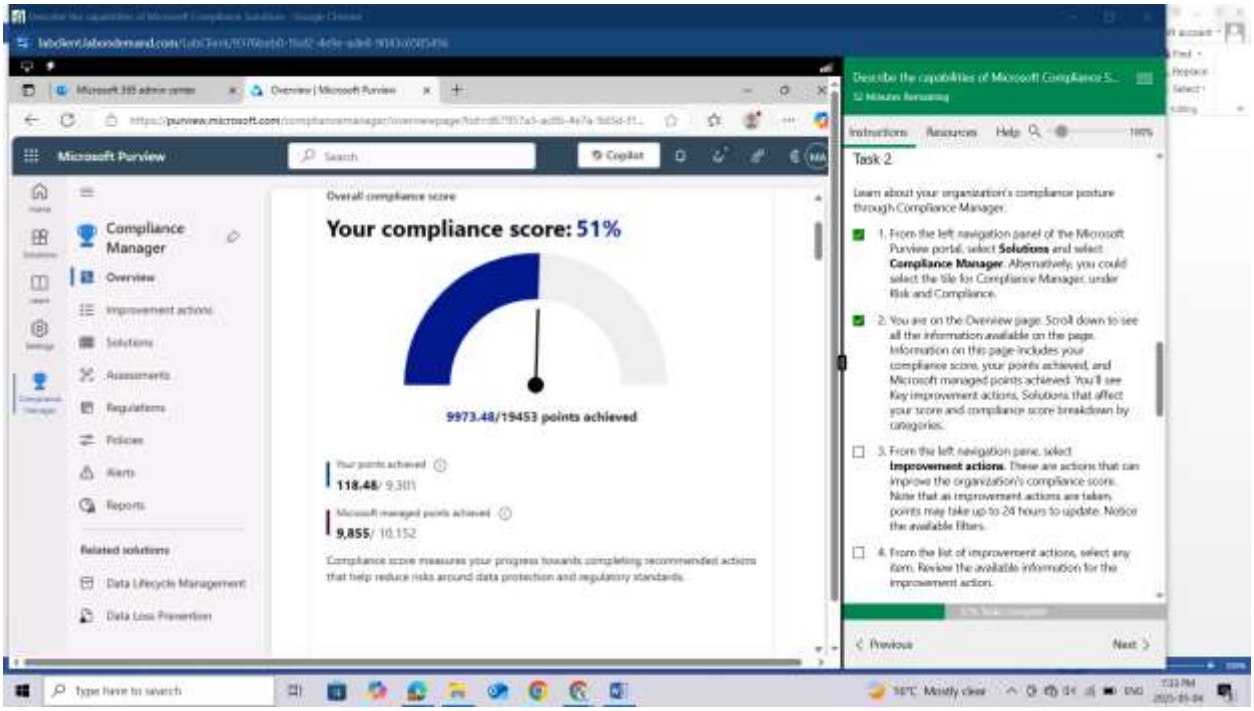



## Task 2

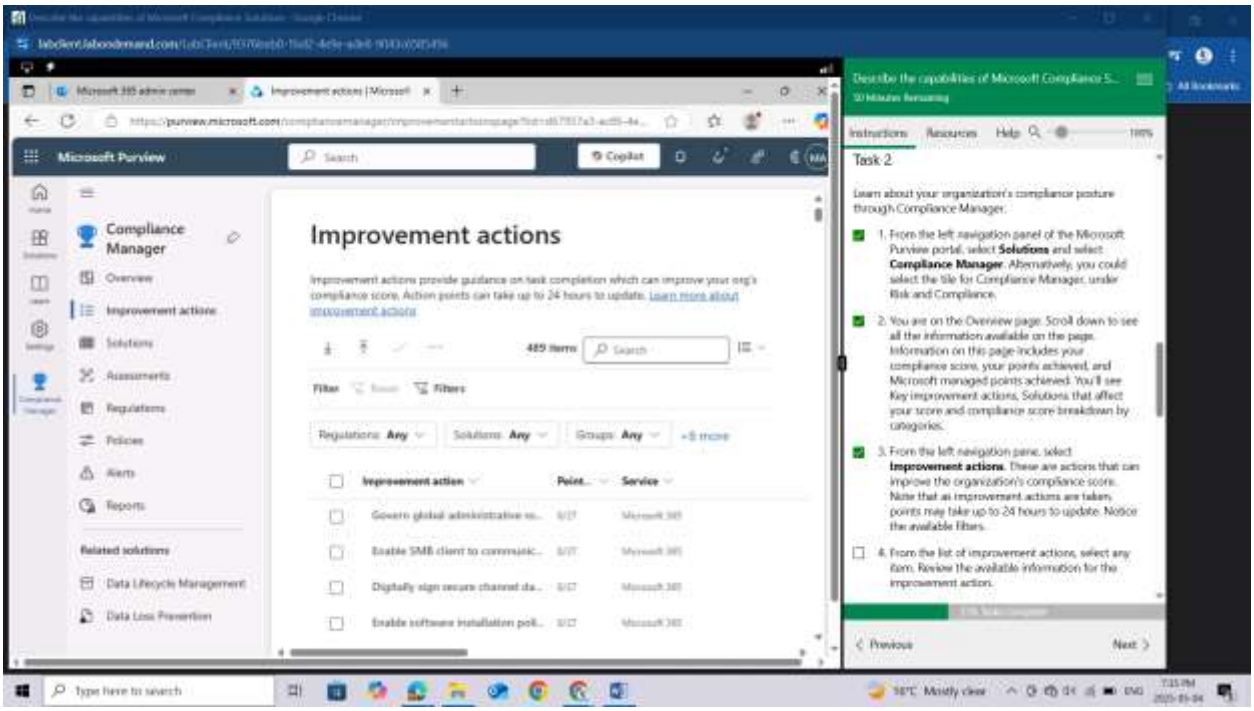
Learn about your organization's compliance posture through Compliance Manager.

From the left navigation panel of the Microsoft Purview portal, select **Solutions** and select **Compliance Manager**. Alternatively, you could select the tile for Compliance Manager, under Risk and Compliance.

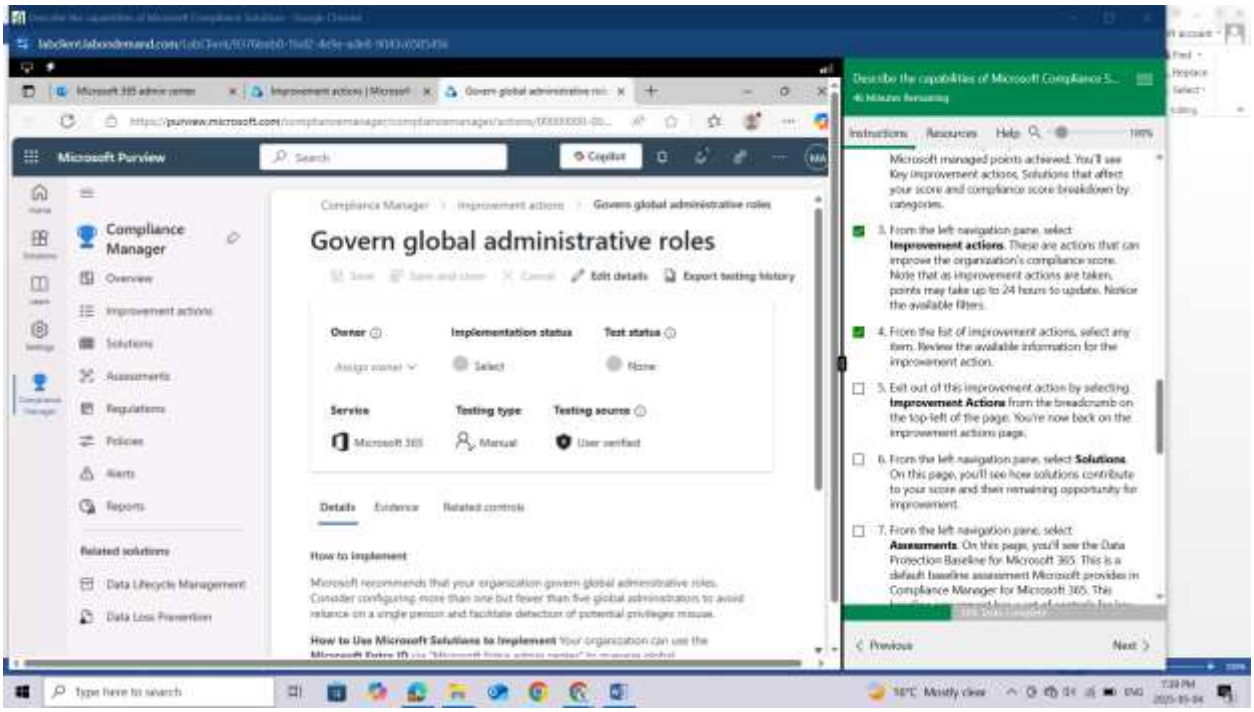
You are on the Overview page. Scroll down to see all the information available on the page. Information on this page includes your compliance score, your points achieved, and Microsoft managed points achieved. You'll see Key improvement actions, Solutions that affect your score and compliance score breakdown by categories.




From the left navigation pane, select **Improvement actions**. These are actions that can improve the organization’s compliance score. Note that as improvement actions are taken, points may take up to 24 hours to update. Notice the available filters.

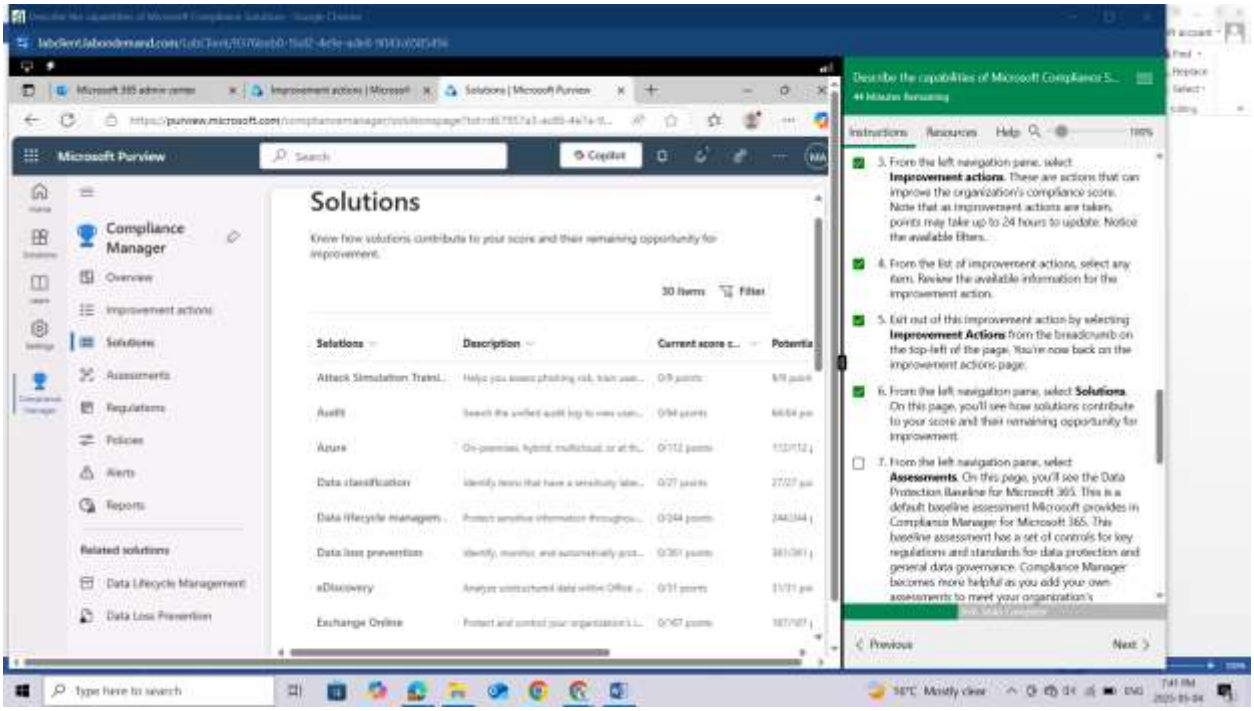



From the list of improvement actions, select any item. Review the available information for the improvement action.

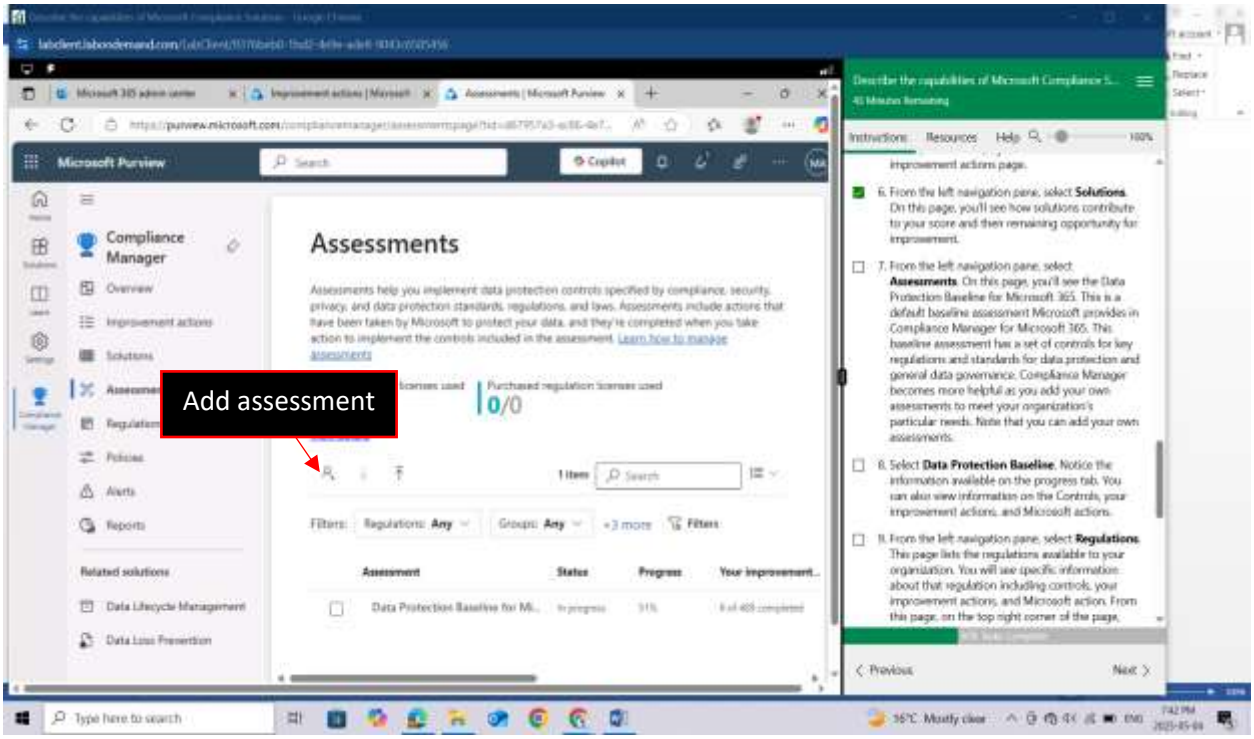



Exit out of this improvement action by selecting Improvement Actions from the breadcrumb on the top-left of the page. You're now back on the improvement actions page.

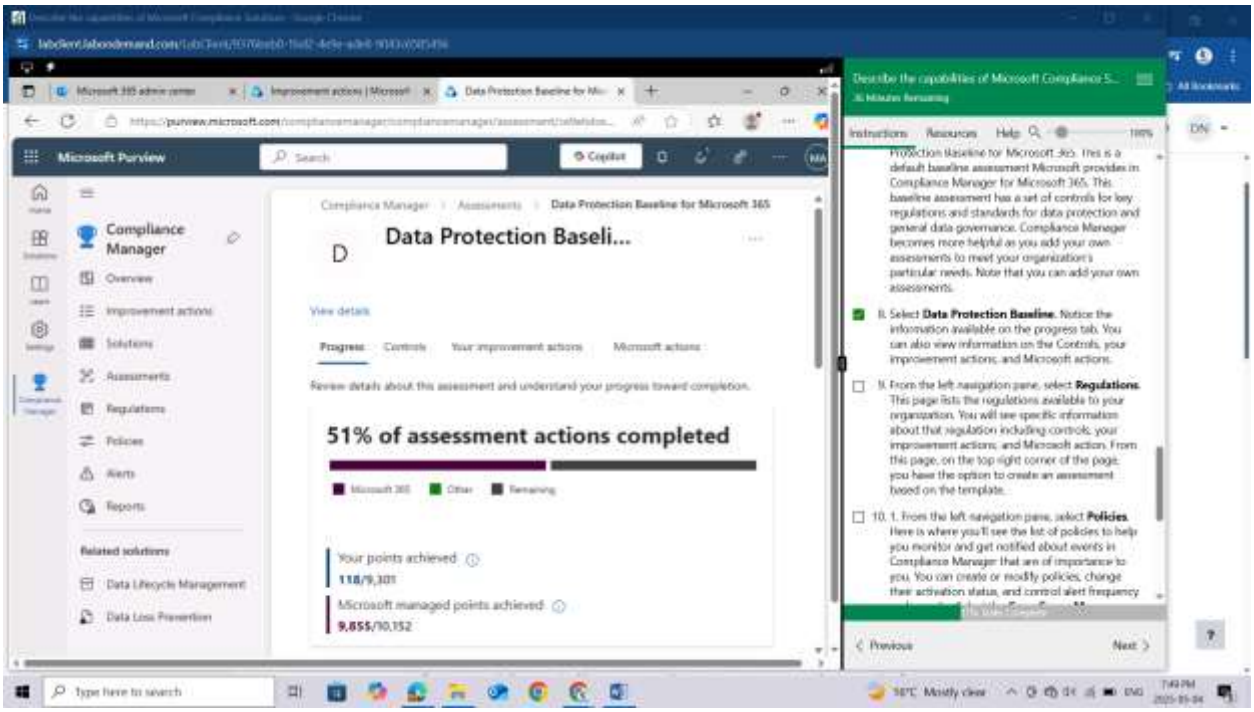
From the left navigation pane, select **Solutions**. On this page, you'll see how solutions contribute to your score and their remaining opportunity for improvement.




From the left navigation pane, select **Assessments**. On this page, you'll see the Data Protection Baseline for Microsoft 365. This is a default baseline assessment Microsoft provides in Compliance Manager for Microsoft 365. This baseline assessment has a set of controls for key regulations and standards for data protection and general data governance. Compliance Manager becomes more helpful as you add your own assessments to meet your organization's particular needs. Note that you can add your own assessments.

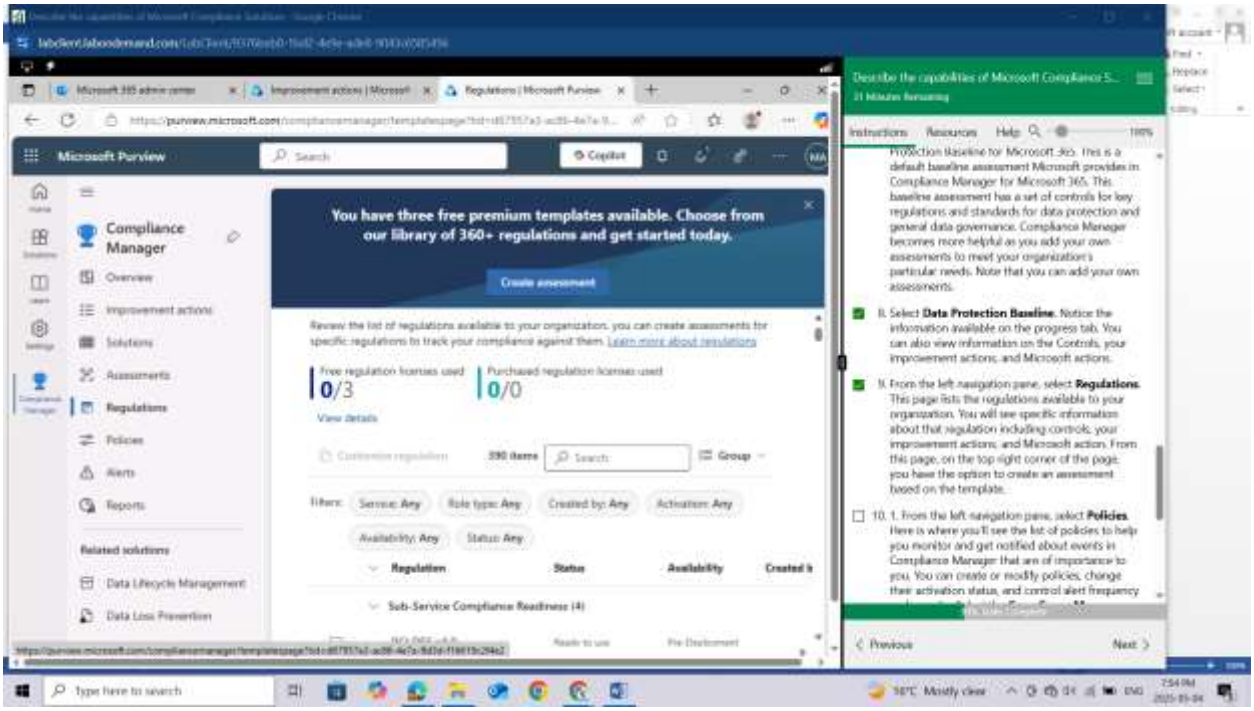



Select **Data Protection Baseline**. Notice the information available on the progress tab. You can also view information on the Controls, your improvement actions, and Microsoft actions.

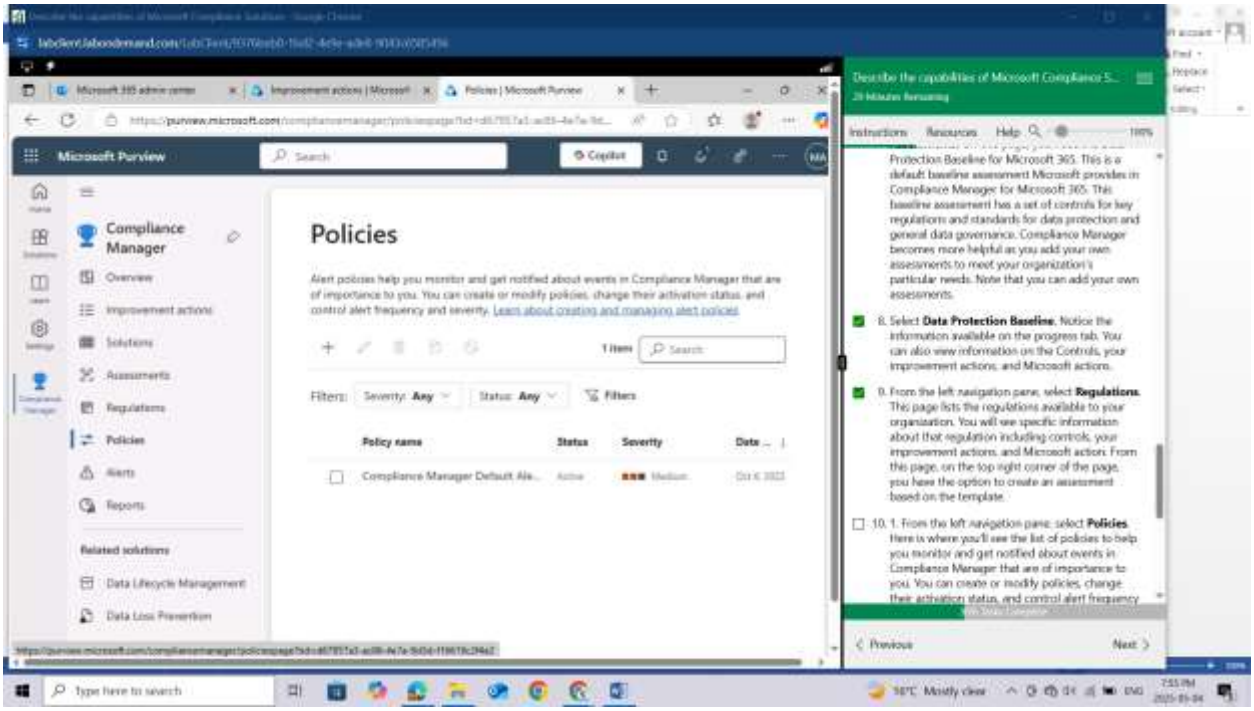


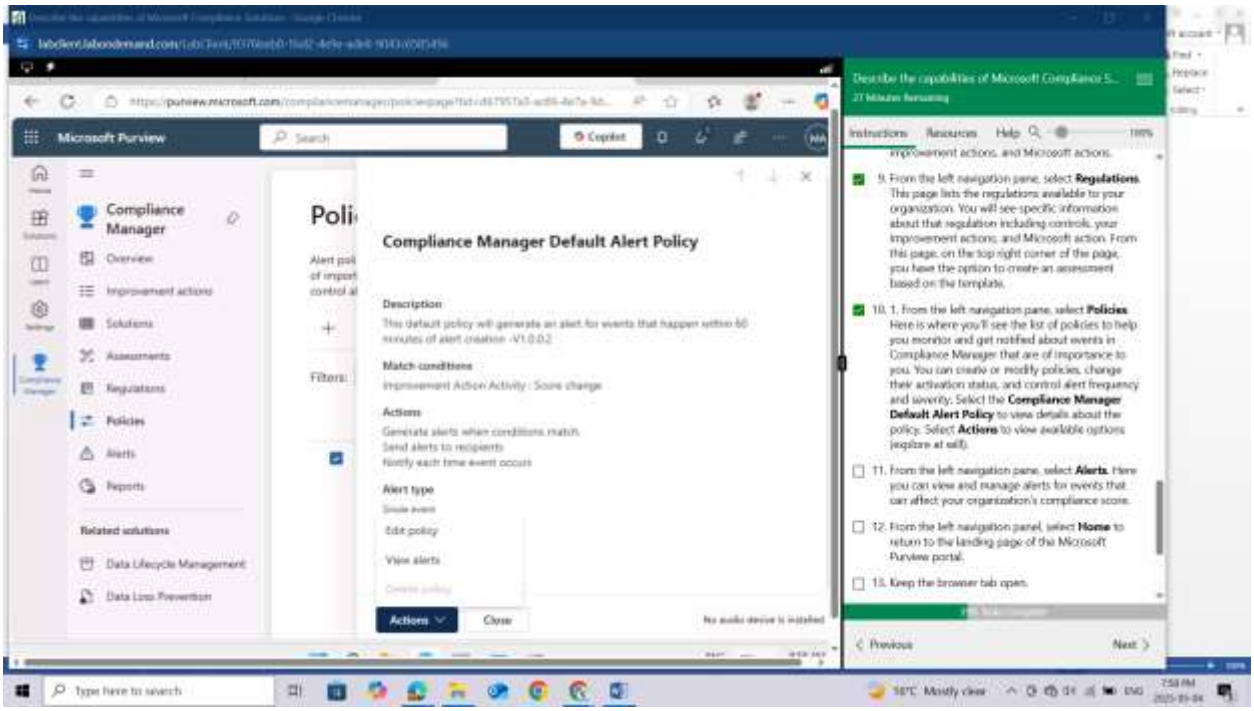

From the left navigation pane, select **Regulations**. This page lists the regulations available to your organization. You will see specific information about that regulation including controls, your

improvement actions, and Microsoft action. From this page, on the top right corner of the page, you have the option to create an assessment based on the template.

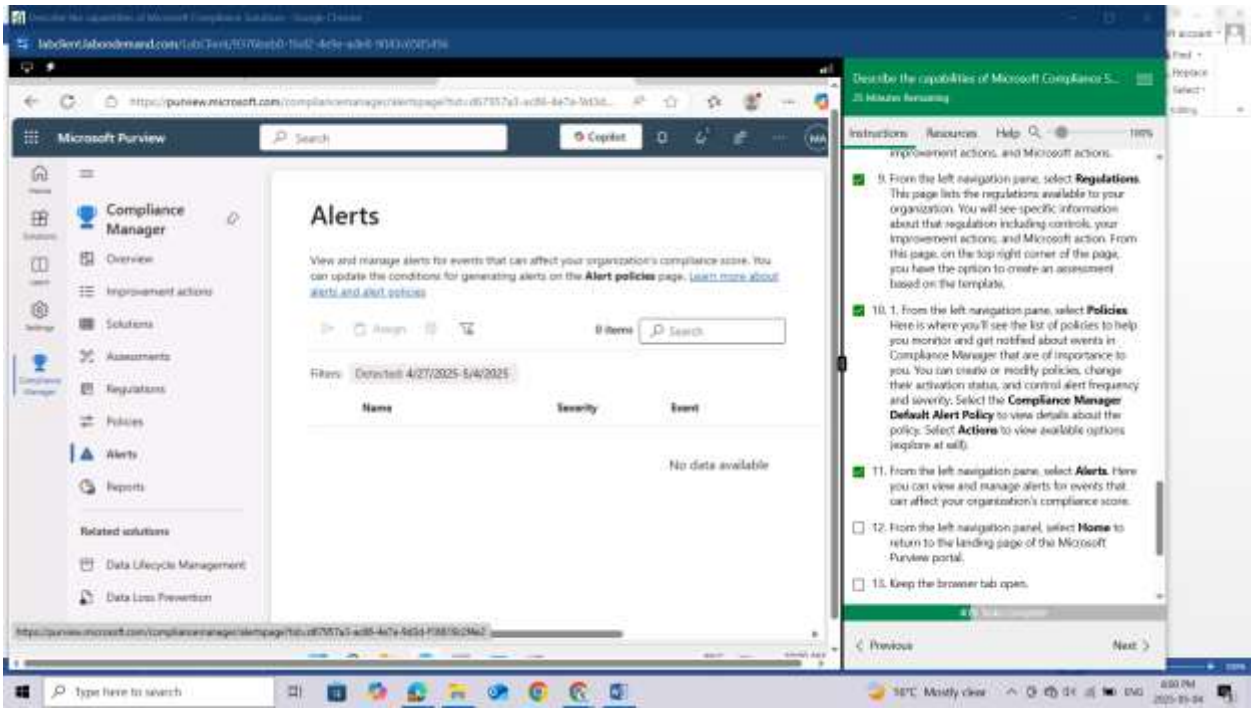



From the left navigation pane, select **Policies**. Here is where you'll see the list of policies to help you monitor and get notified about events in Compliance Manager that are of importance to you. You can create or modify policies, change their activation status, and control alert frequency and severity. Select the Compliance Manager Default Alert Policy to view details about the policy. Select **Actions** to view available options (explore at will).



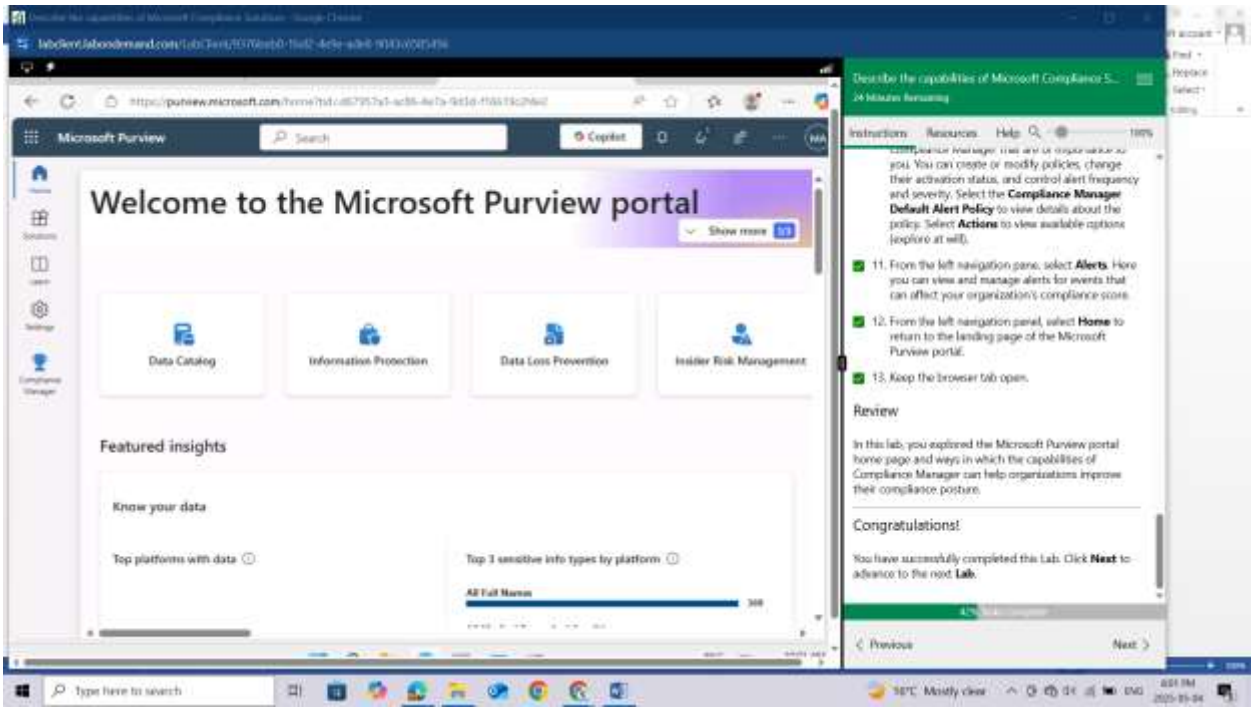



From the left navigation pane, select **Alerts**. Here you can view and manage alerts for events that can affect your organization's compliance score.




From the left navigation panel, select **Home** to return to the landing page of the Microsoft Purview portal.

Keep the browser tab open.




## Review

In this lab, you explored the Microsoft Purview portal home page and ways in which the capabilities of Compliance Manager can help organizations improve their compliance posture.

# 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.

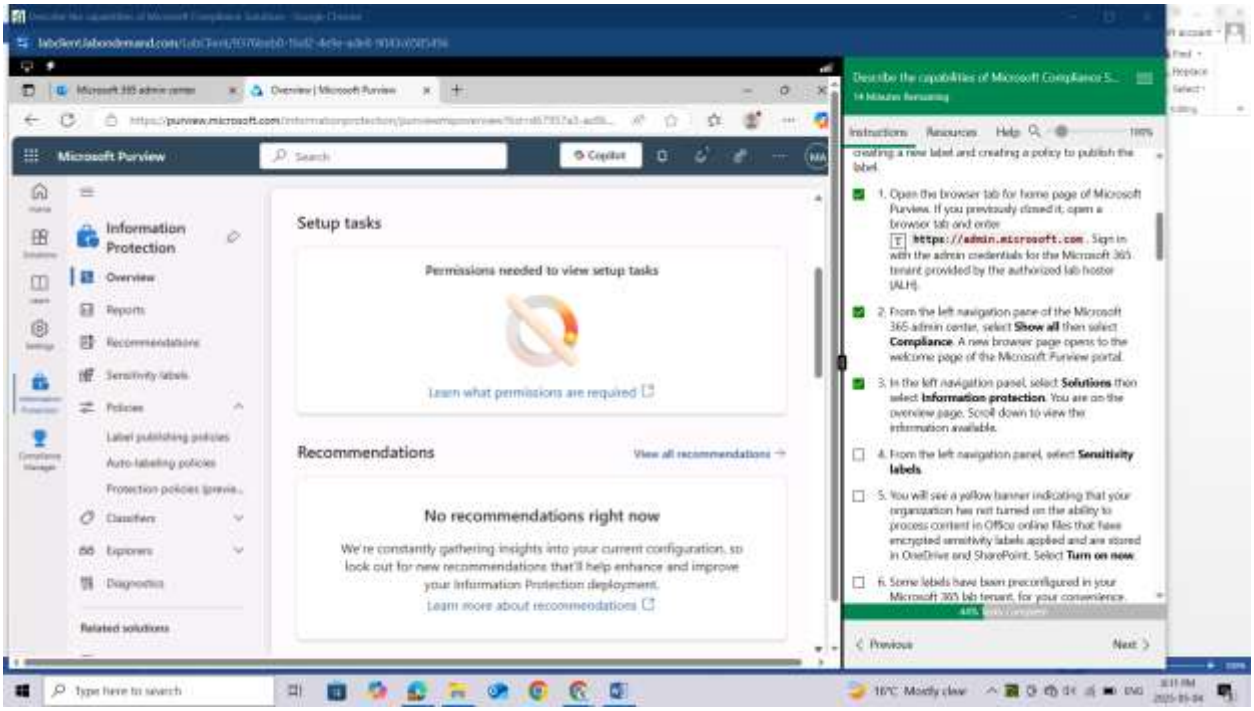
## Task 1

In this task, you'll gain an understanding of what sensitivity labels can do by going through the process of creating a new label and creating a policy to publish the label.

Open the browser tab for home page of Microsoft Purview. If you previously closed it, open a browser tab and enter https://admin.microsoft.com. Sign in with the admin credentials for the Microsoft 365 tenant provided by the authorized lab hoster (ALH).

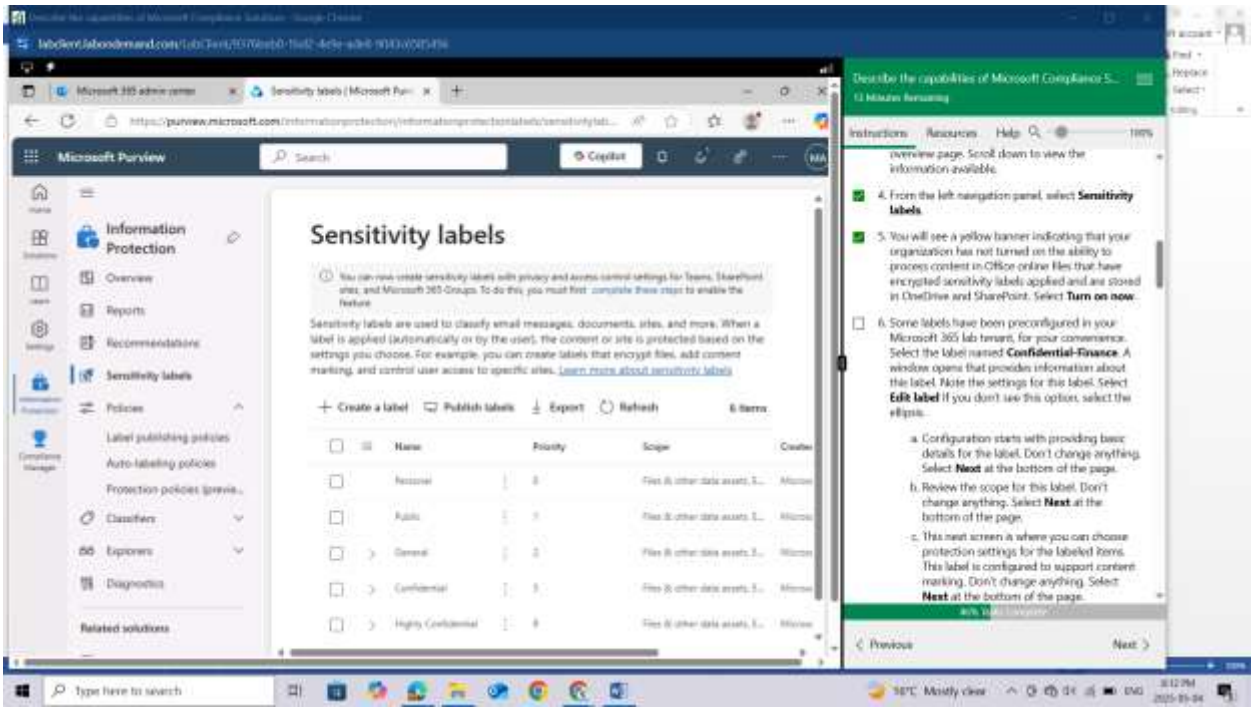
From the left navigation pane of the Microsoft 365 admin center, select Show all then select Compliance. A new browser page opens to the welcome page of the Microsoft Purview portal.

In the left navigation panel, select Solutions then select **Information protection**. You are on the overview page. Scroll down to view the information available.

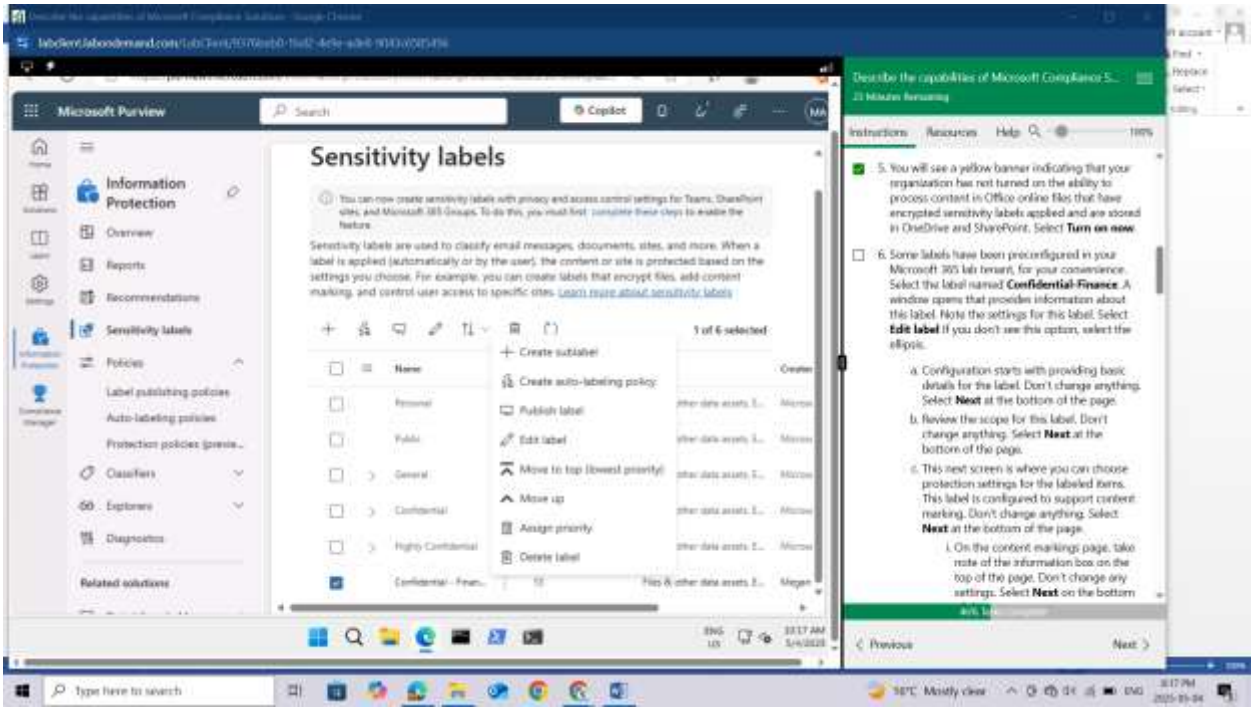



From the left navigation panel, select **Sensitivity labels.**

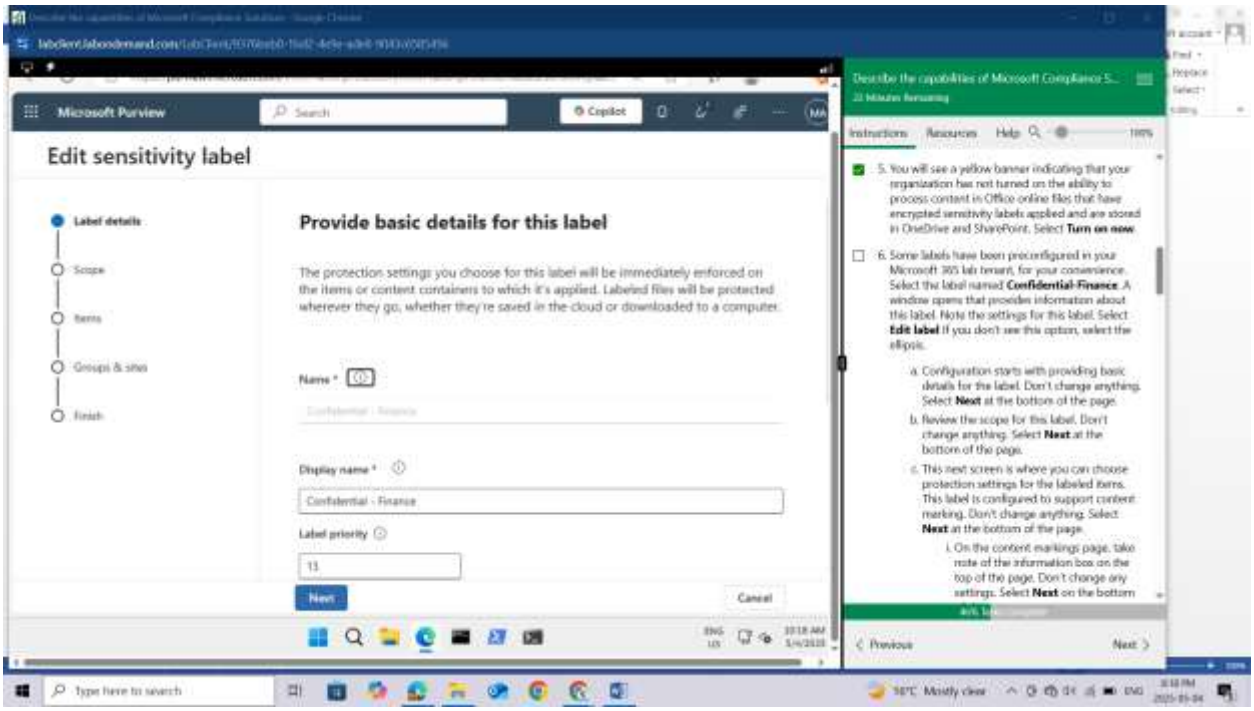
You will see a yellow banner indicating that your organization has not turned on the ability to process content in Office online files that have encrypted sensitivity labels applied and are stored in OneDrive and SharePoint. Select **Turn on now.**



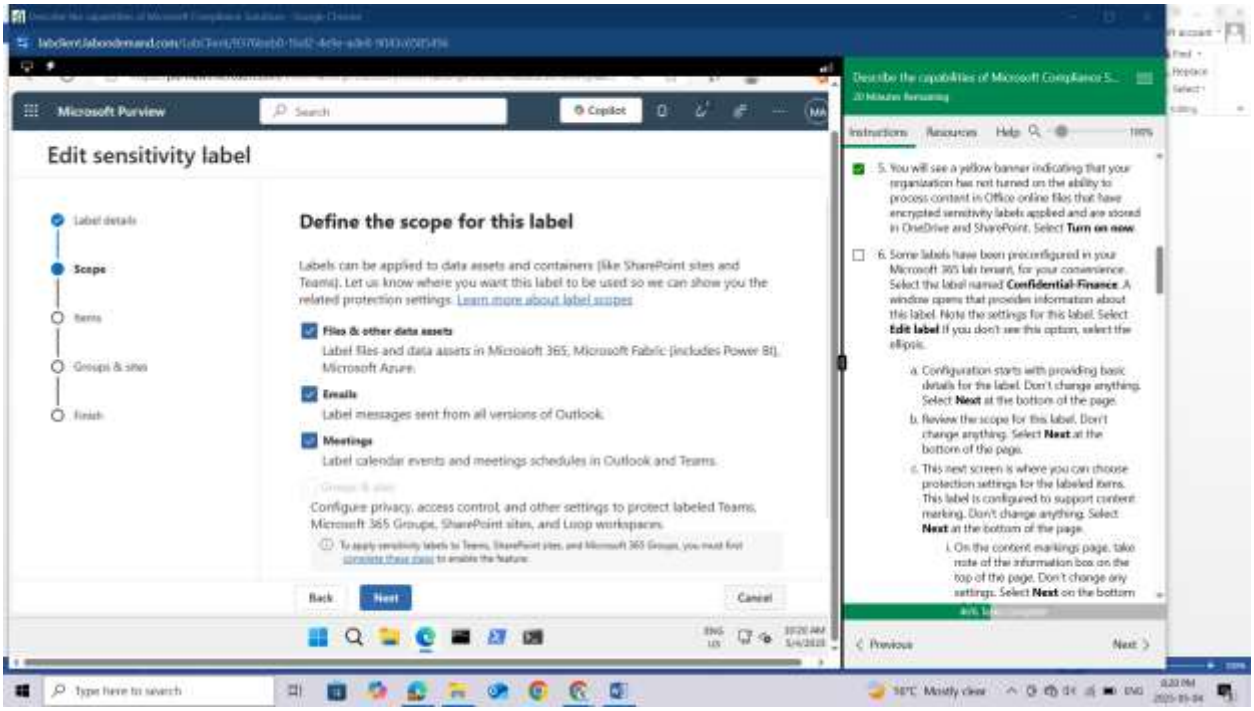

Some labels have been preconfigured in your Microsoft 365 lab tenant, for your convenience. Select the label named **Confidential-Finance.** A window opens that provides information about this label. Note the settings for this label. Select **Edit label** If you don't see this option, select the ellipsis.




Configuration starts with providing basic details for the label. Don’t change anything. Select **Next** at the bottom of the page.

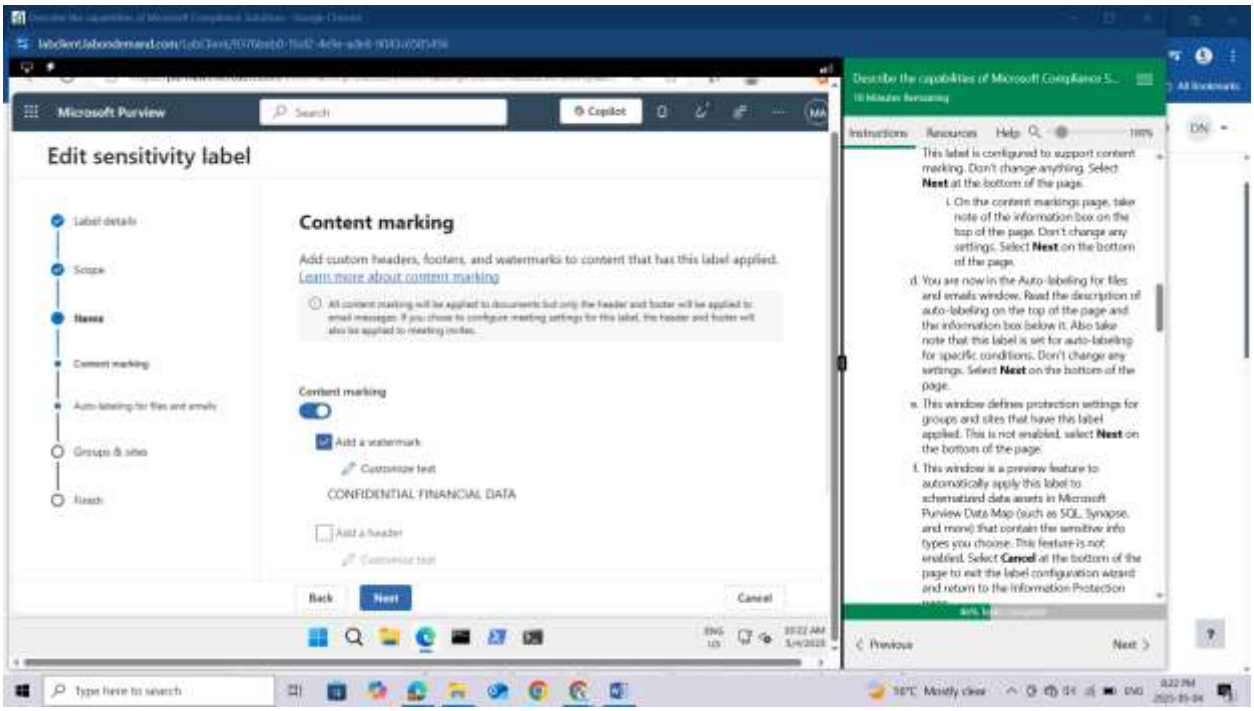



Review the scope for this label. Don't change anything. Select **Next** at the bottom of the page.

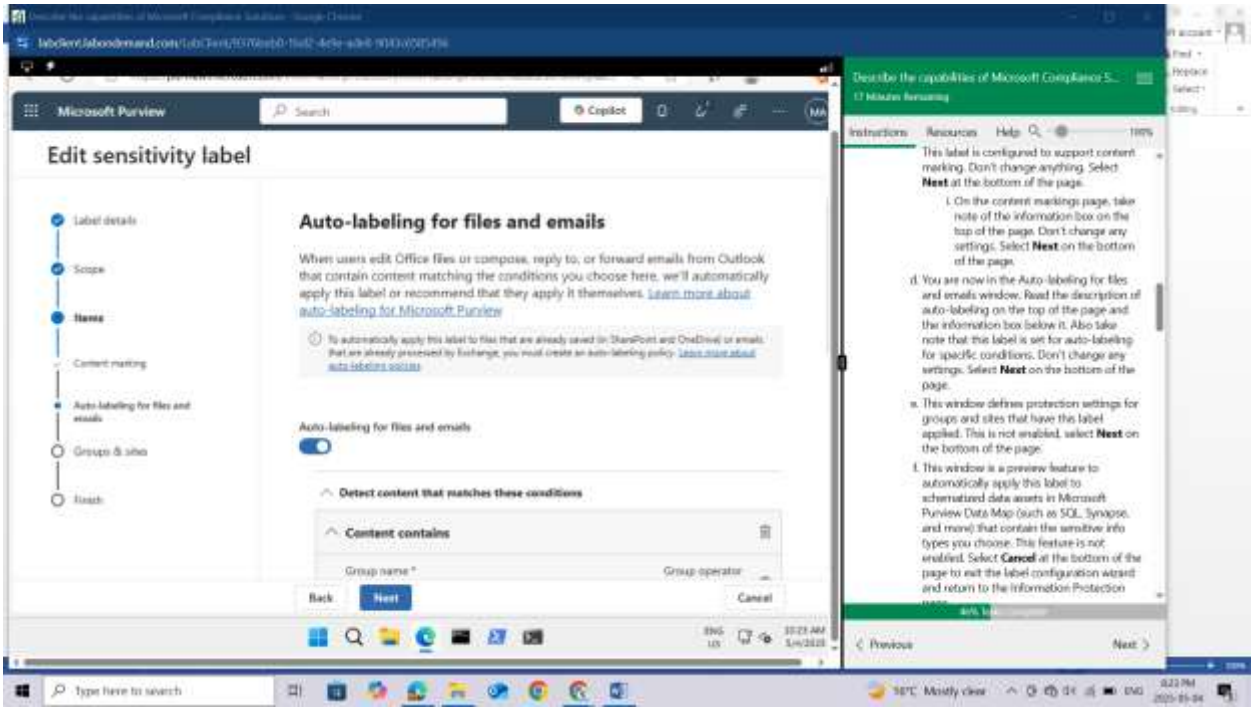



This next screen is where you can choose protection settings for the labeled items. This label is configured to support content marking. Don't change anything. Select **Next** at the bottom of the page.

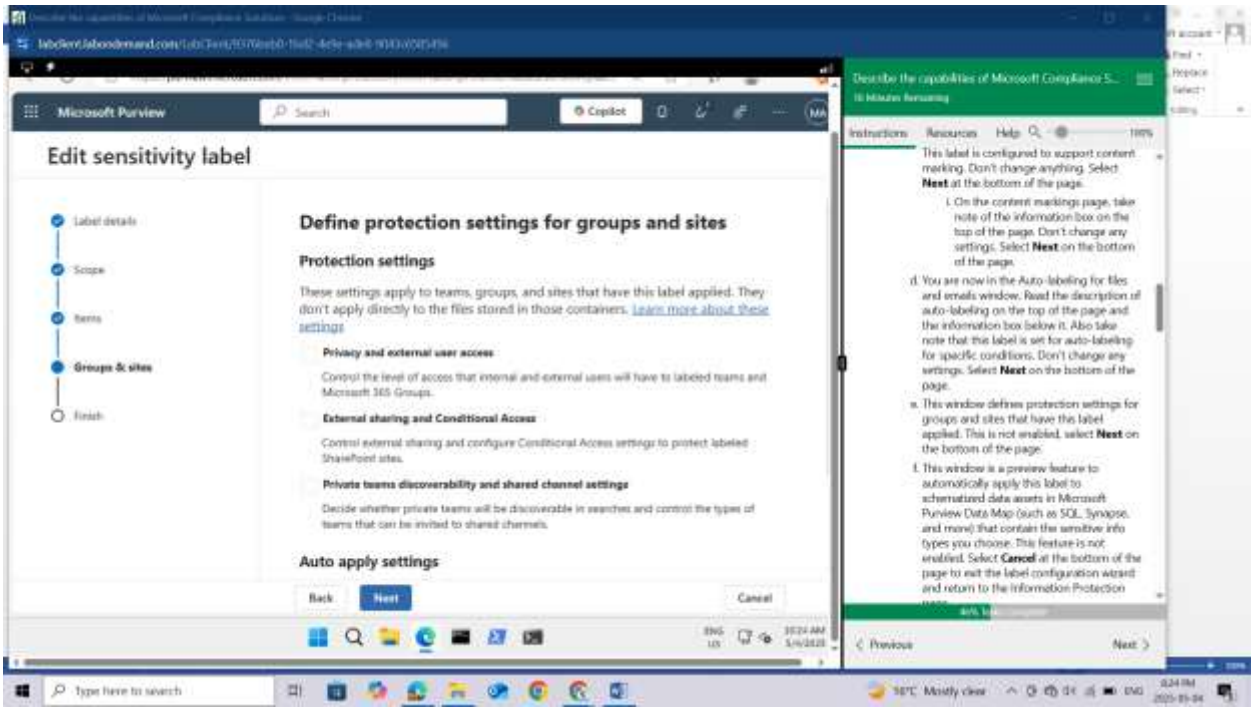
On the content markings page, take note of the information box on the top of the page. Don't change any settings. Select **Next** on the bottom of the page.



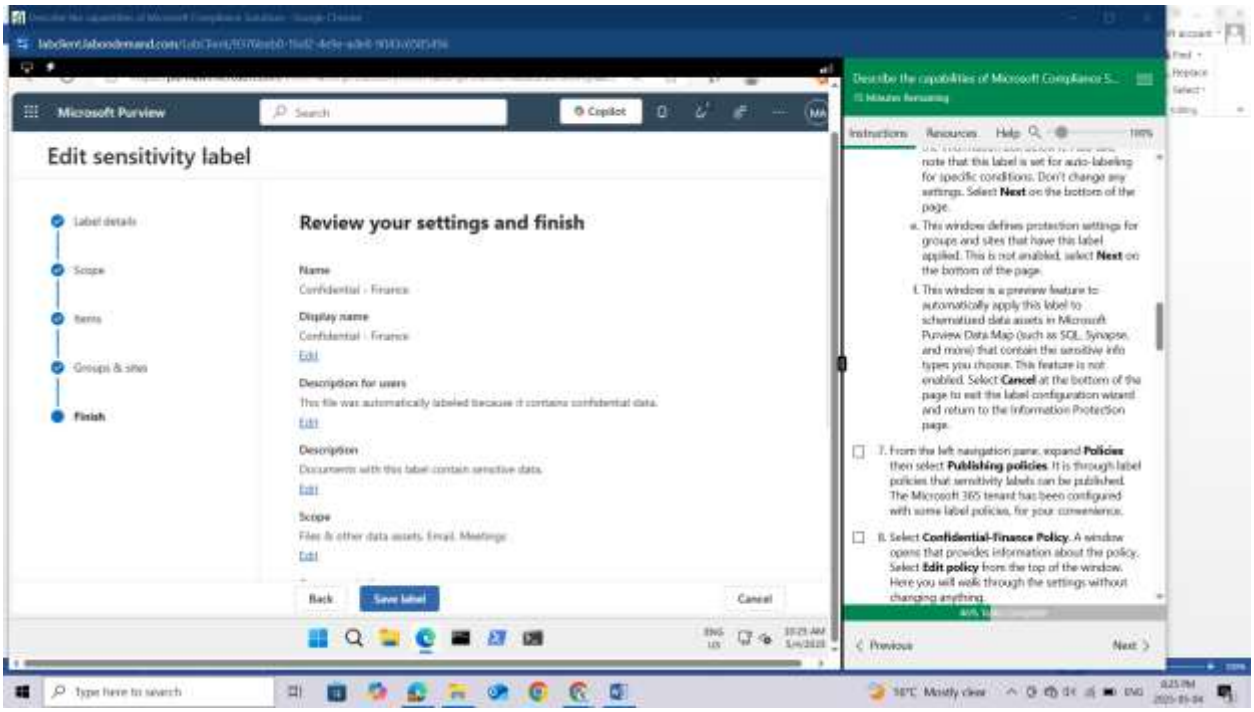

You are now in the Auto-labeling for files and emails window. Read the description of auto-labeling on the top of the page and the information box below it. Also take note that this label is set for auto-labeling for specific conditions. Don't change any settings. Select **Next** on the bottom of the page.




This window defines protection settings for groups and sites that have this label applied. This is not enabled, select **Next** on the bottom of the page.

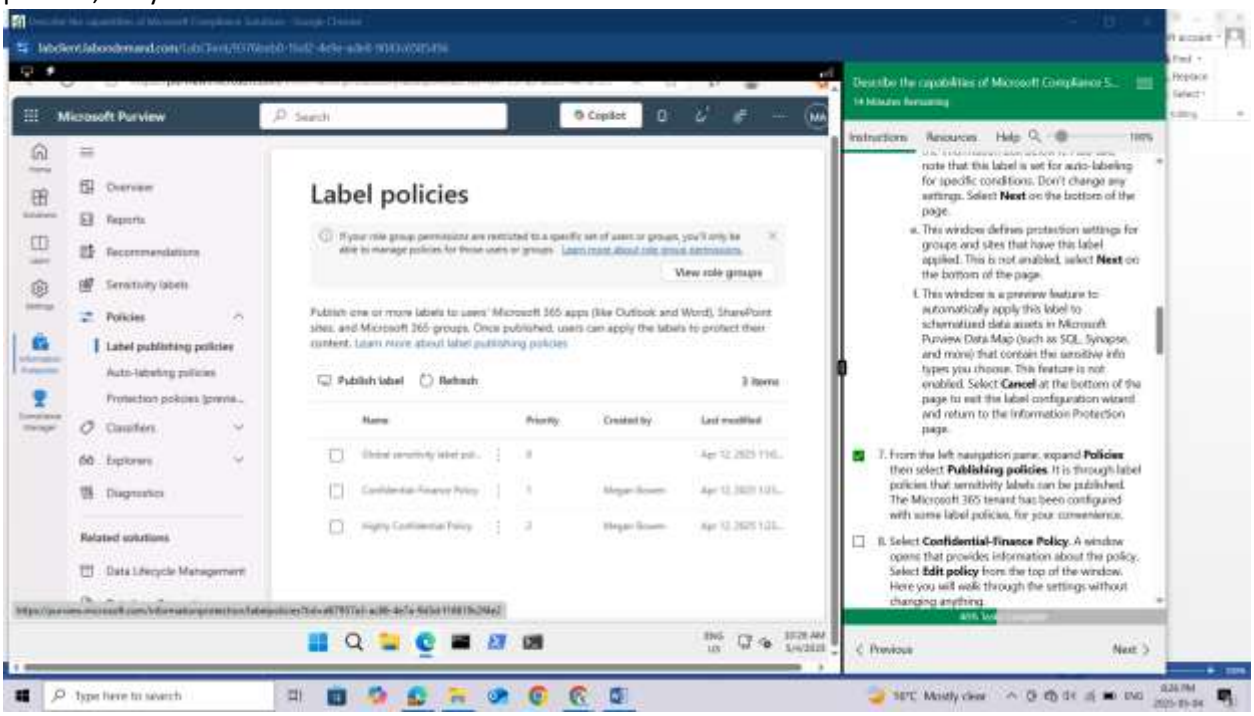



This window is a preview feature to automatically apply this label to schematized data assets in Microsoft Purview Data Map (such as SQL, Synapse, and more) that contain the sensitive info types you choose. This feature is not enabled. Select **Cancel** at the bottom of the page to exit the label configuration wizard and return to the Information Protection page.



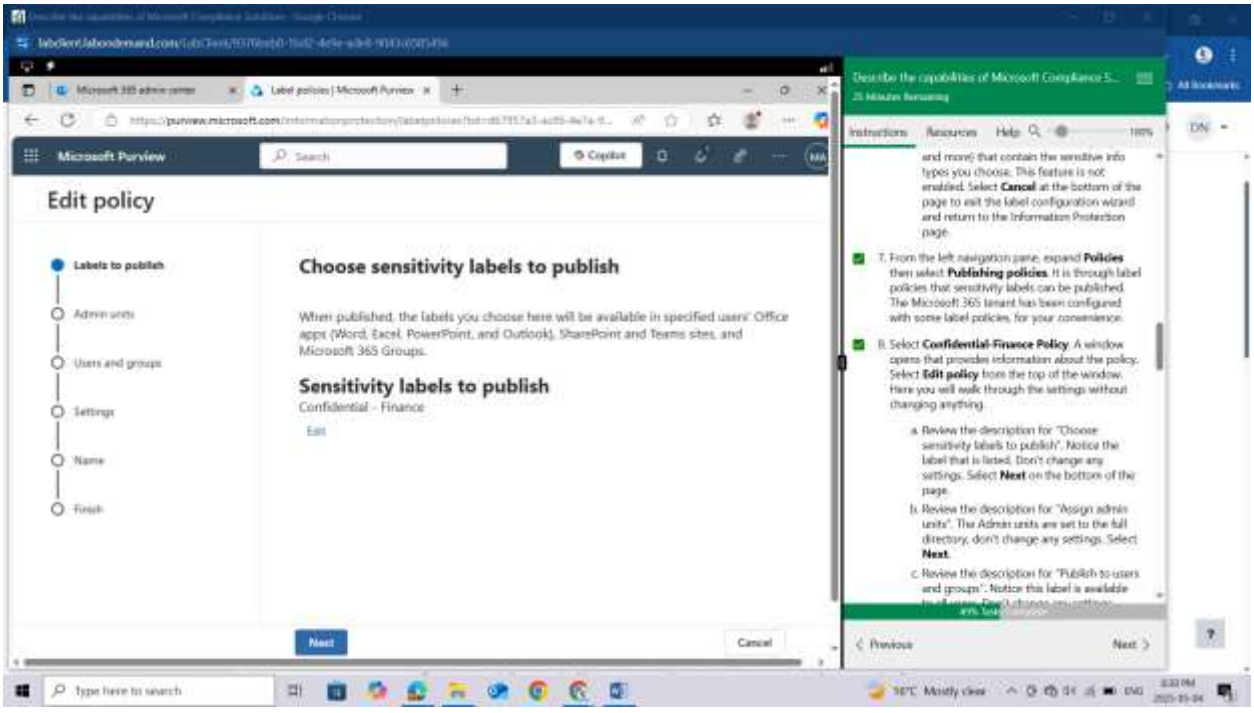

From the left navigation pane, expand **Policies** then select **Publishing policies**. It is through label policies that sensitivity labels can be published. The Microsoft 365 tenant has been configured with some label

policies, for your convenience.

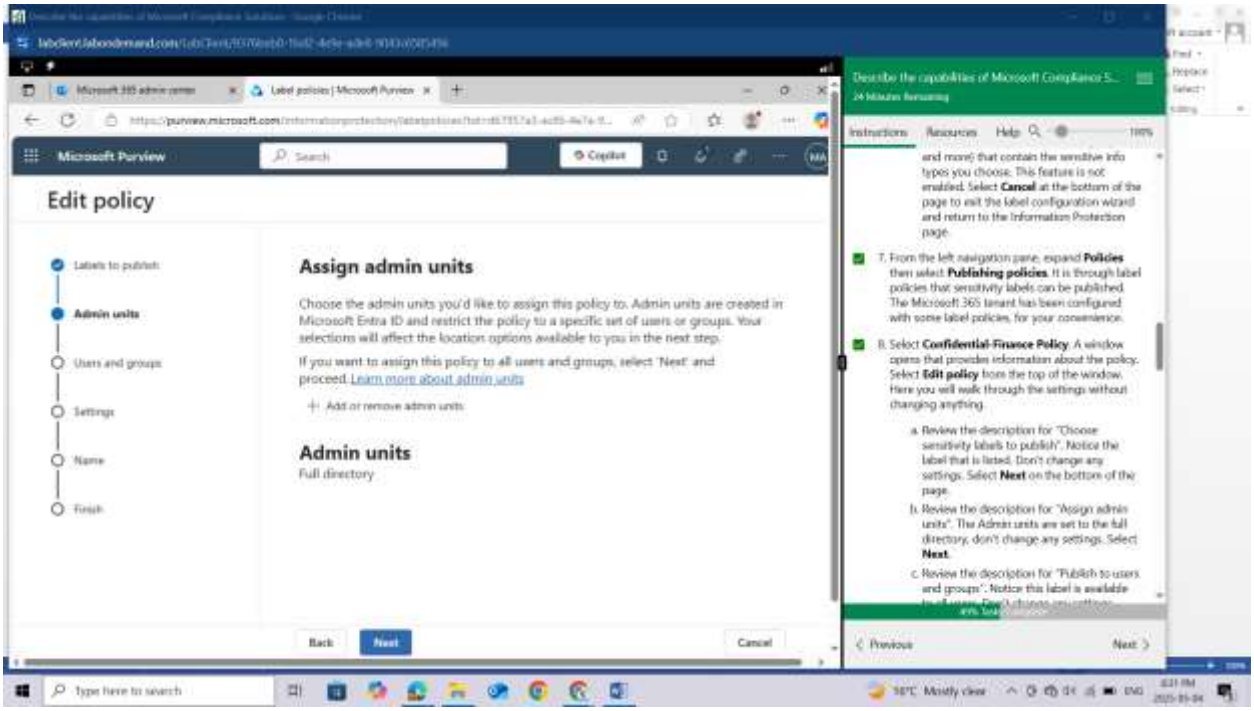



Select **Confidential-Finance Policy**. A window opens that provides information about the policy. Select **Edit policy** from the top of the window. Here you will walk through the settings without changing anything.

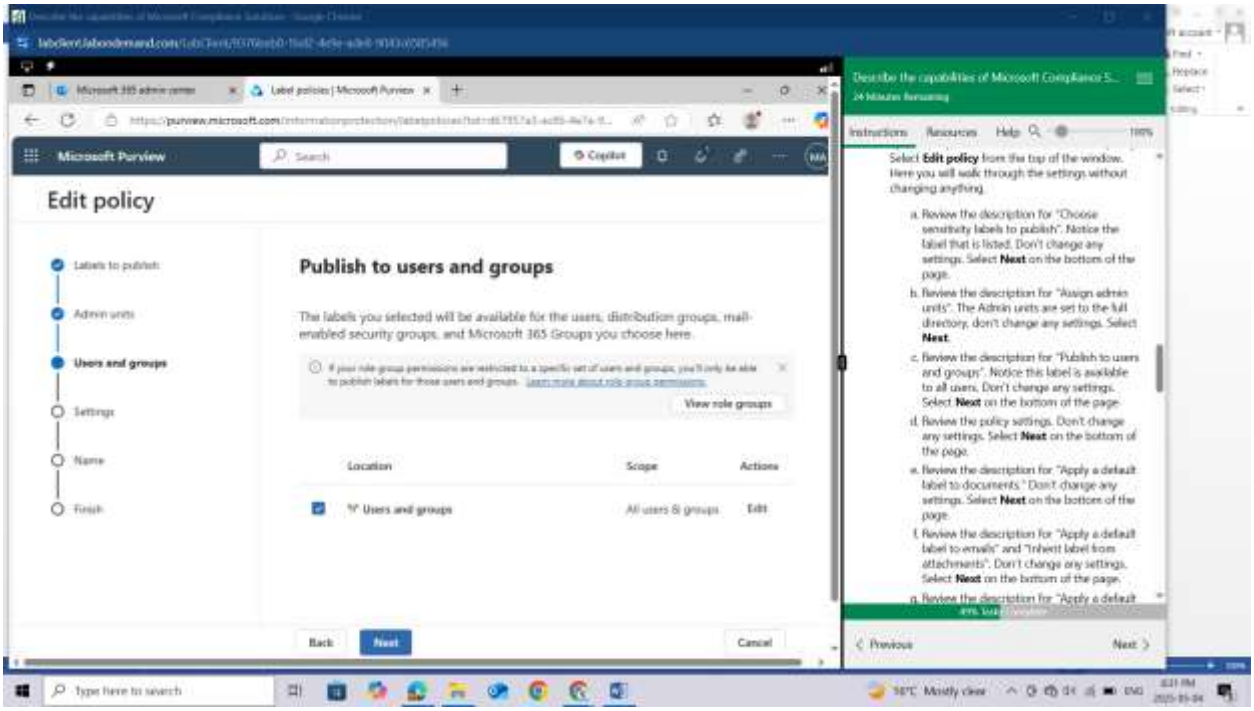
Review the description for “Choose sensitivity labels to publish”. Notice the label that is listed. Don’t change any settings. Select **Next** on the bottom of the page.



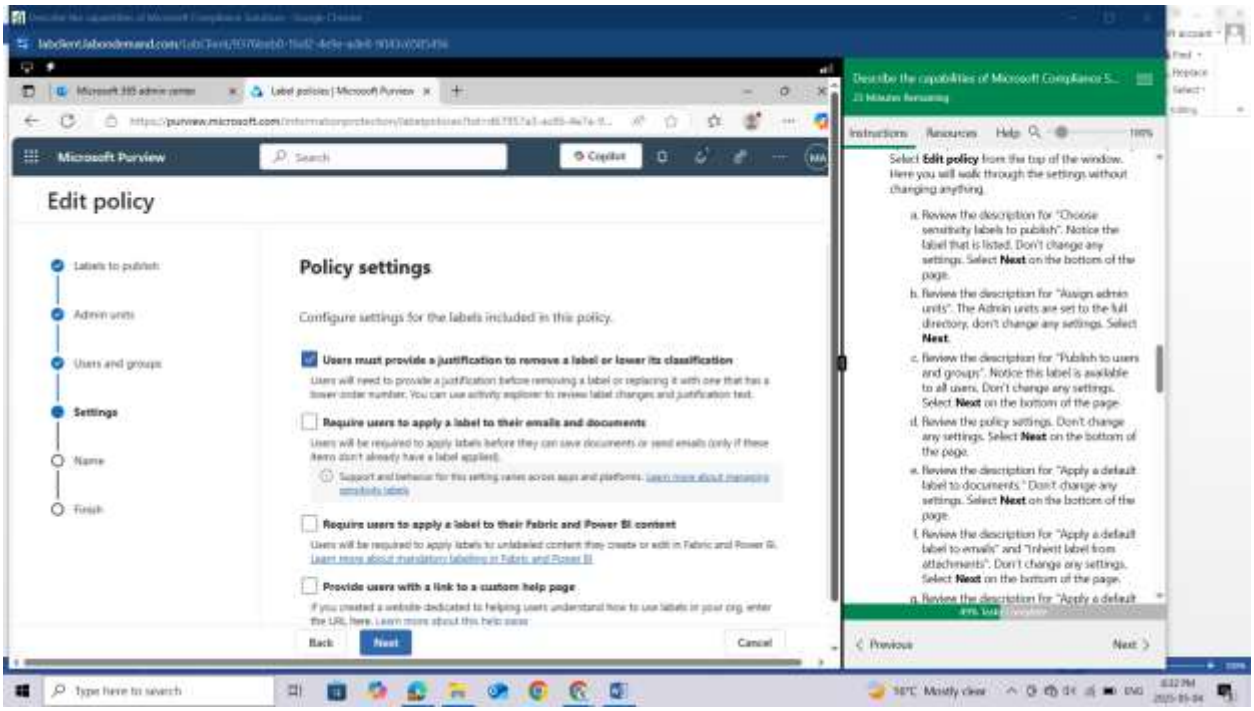
Review the description for "Assign admin units". The Admin units are set to the full directory, don't change any settings. Select **Next**.



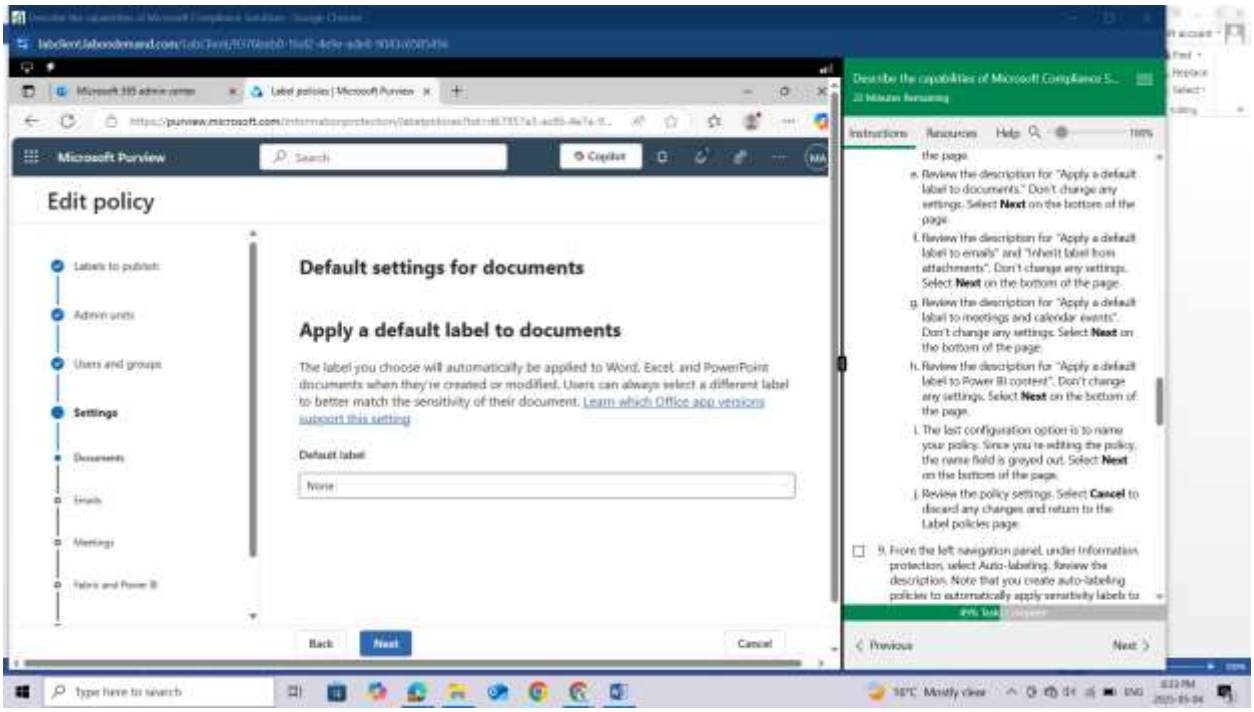

Review the description for “Publish to users and groups”. Notice this label is available to all users. Don’t change any settings. Select **Next** on the bottom of the page.



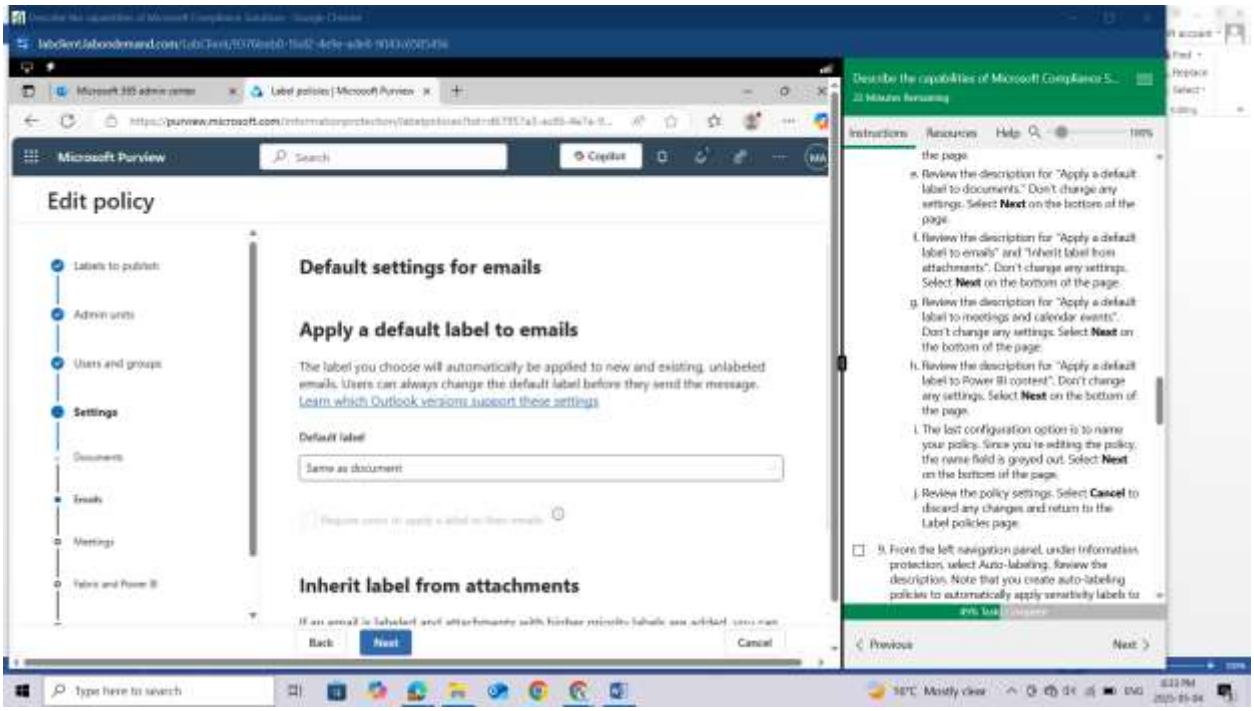

Review the policy settings. Don’t change any settings. Select **Next** on the bottom of the page.



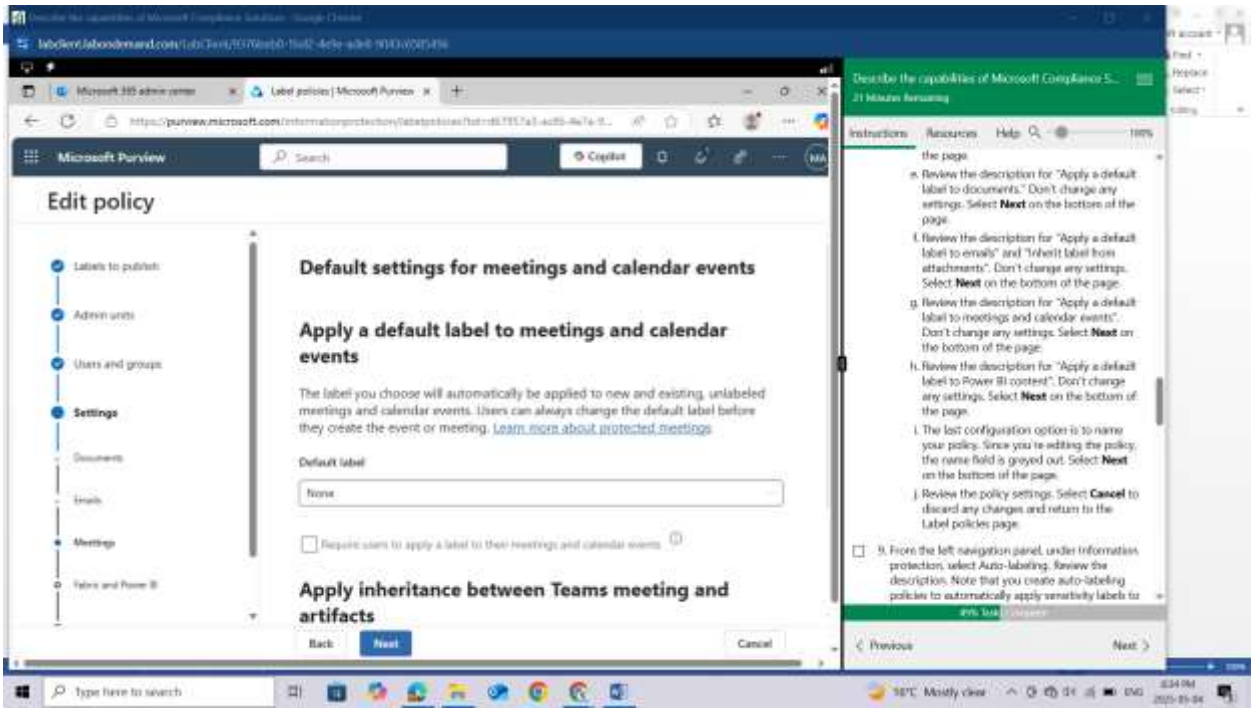

Review the description for "Apply a default label to documents." Don’t change any settings. Select **Next** on the bottom of the page.



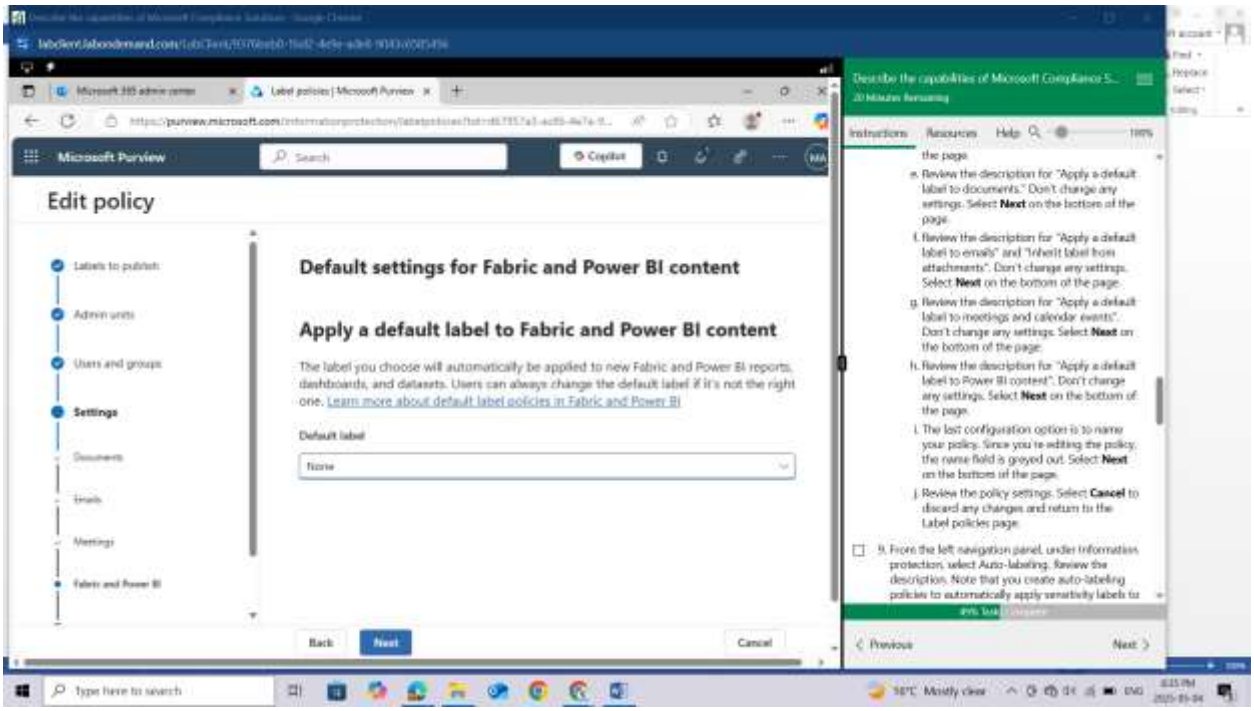

Review the description for "Apply a default label to emails" and "Inherit label from attachments". Don’t change any settings. Select **Next** on the bottom of the page.



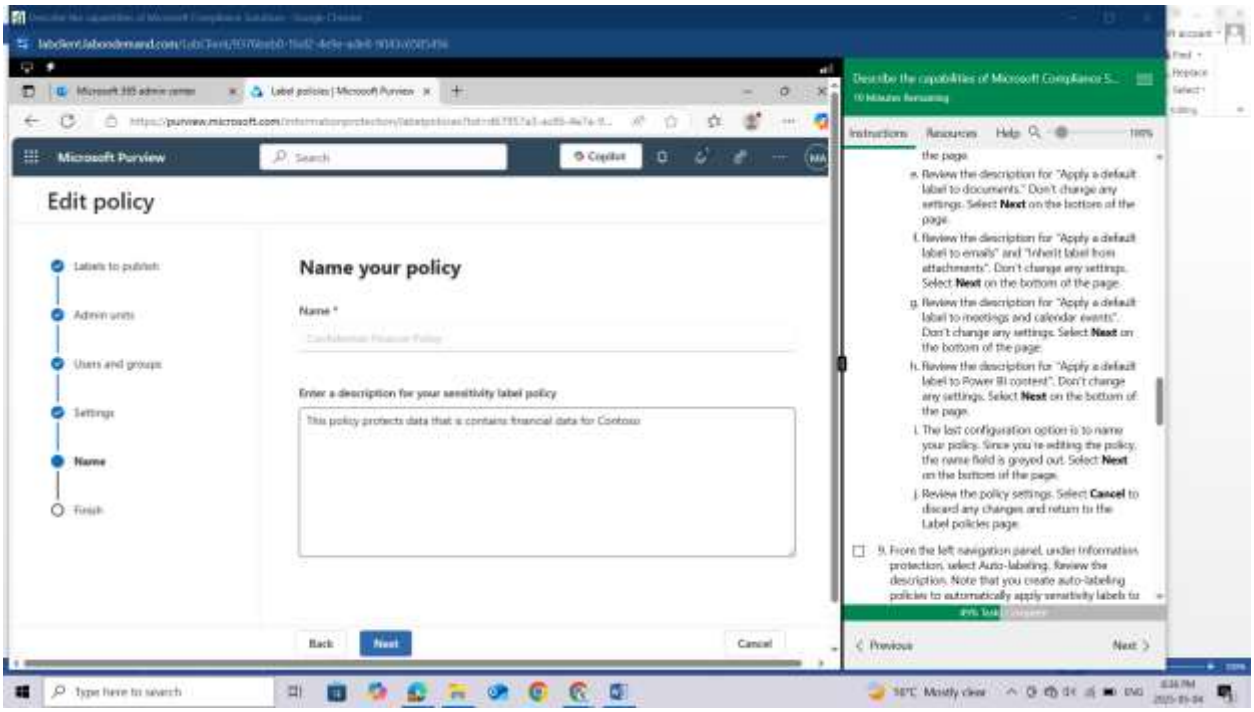

Review the description for "Apply a default label to meetings and calendar events". Don’t change any settings. Select **Next** on the bottom of the page.



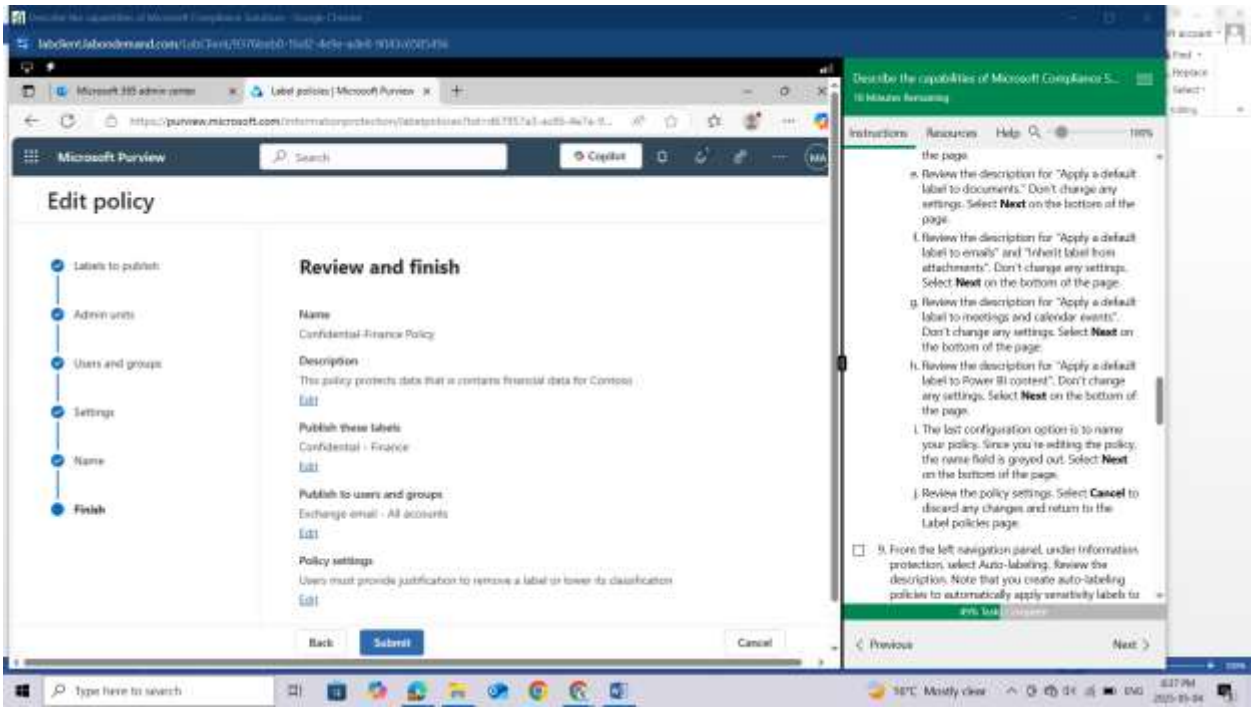

Review the description for "Apply a default label to Power BI content". Don’t change any settings. Select **Next** on the bottom of the page.



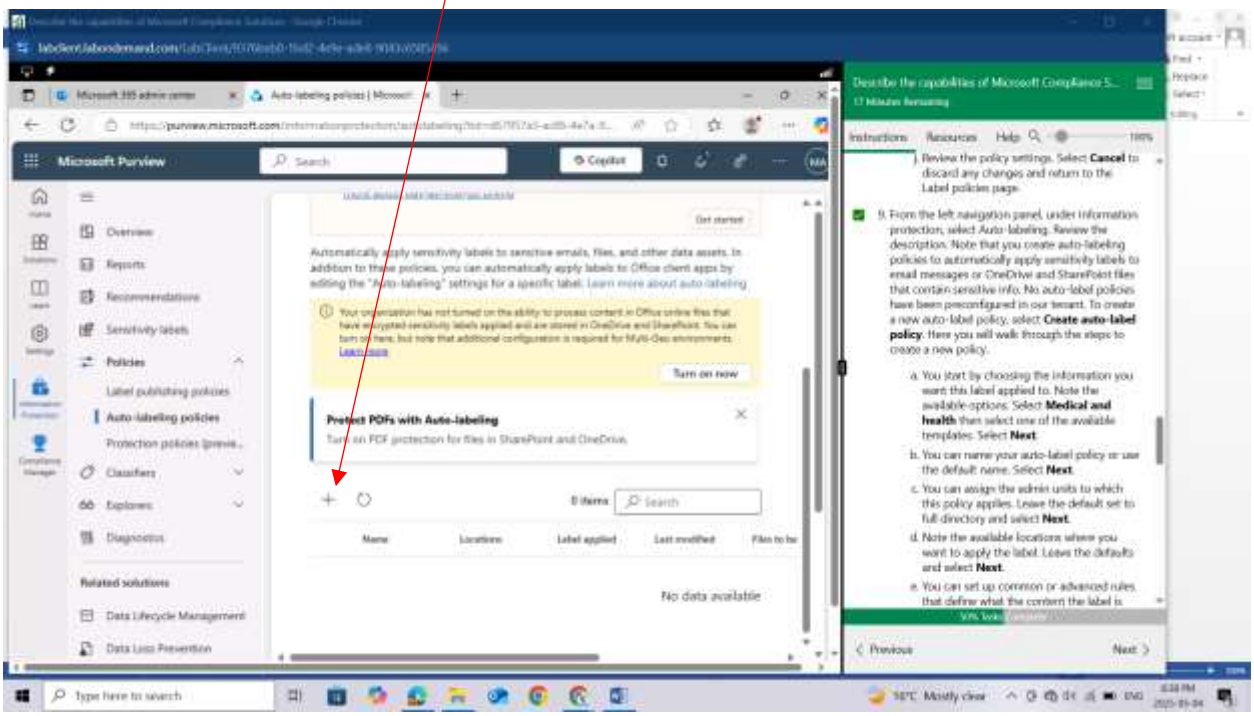

The last configuration option is to name your policy. Since you're editing the policy, the name field is greyed out. Select **Next** on the bottom of the page.



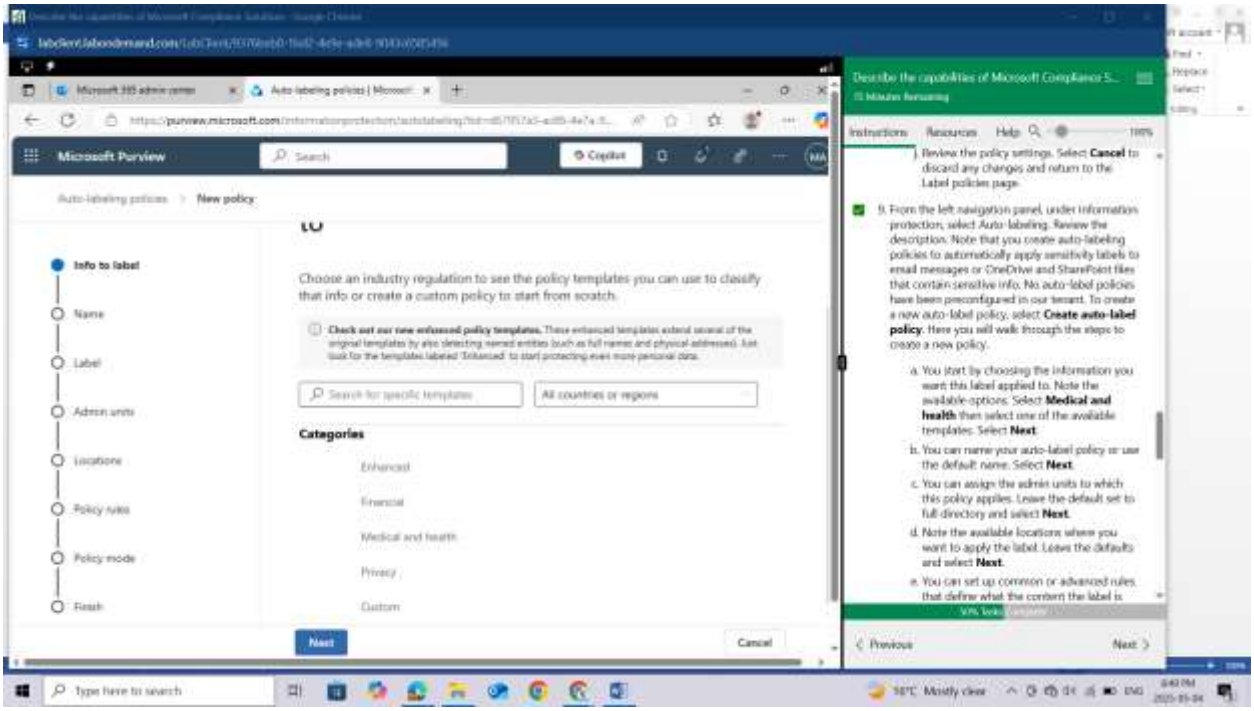

Review the policy settings. Select **Cancel** to discard any changes and return to the Label policies page.



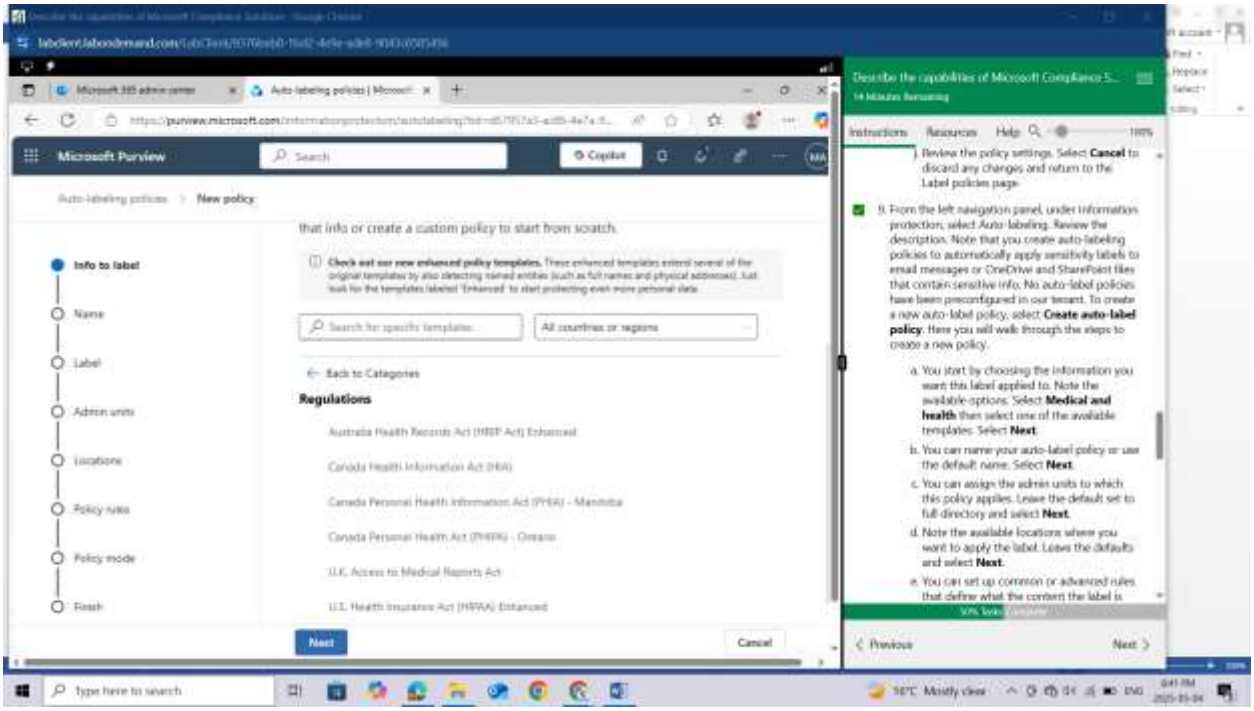

From the left navigation panel, under Information protection, select **Auto-labeling.** Review the description. Note that you create auto-labeling policies to automatically apply sensitivity labels to email messages or OneDrive and SharePoint files that contain sensitive info. No auto-label policies 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.



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**.




You can name your auto-label policy or use the default name. Select **Next**.

You can assign the admin units to which this policy applies. Leave the default set to full directory and select **Next**.

Note the available locations where you want to apply the label. Leave the defaults and select **Next**.

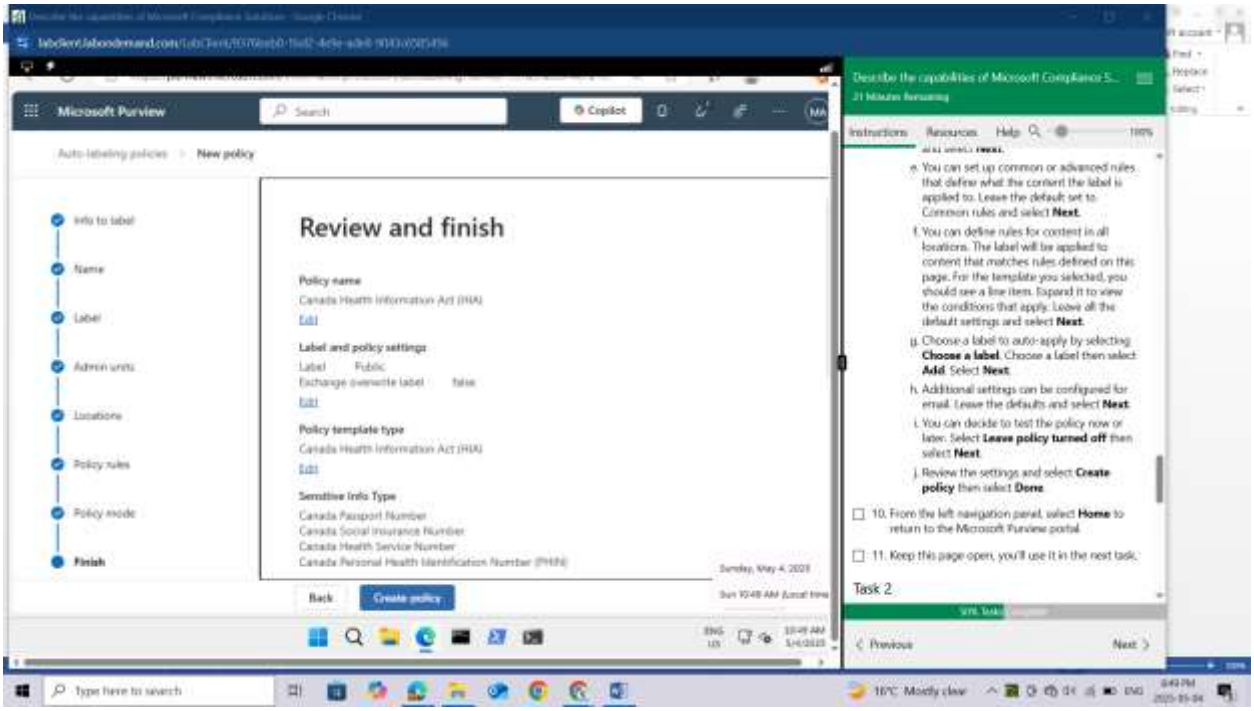
You can set up common or advanced rules that define what the content the label is applied to. Leave the default set to Common rules and select **Next**.

You can define rules for content in all locations. The label will be applied to content that matches rules defined on this page. For the template you selected, you should see a line item. Expand it to view the conditions that apply. Leave all the default settings and select **Next**.

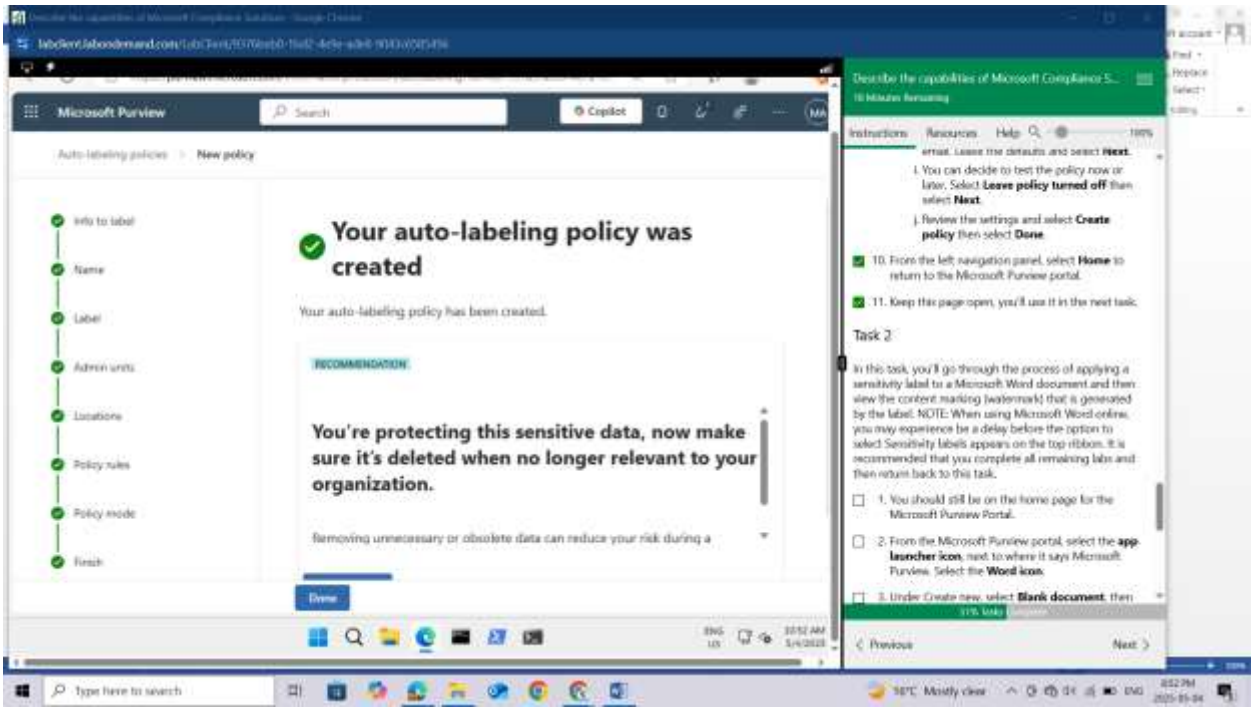
Choose a label to auto-apply by selecting Choose a label. Choose a label then select **Add**. Select **Next**.

Additional settings can be configured for email. Leave the defaults and select **Next**.

You can decide to test the policy now or later. Select Leave policy turned off then select **Next**.




Review the settings and select **Create policy** then select **Done**.



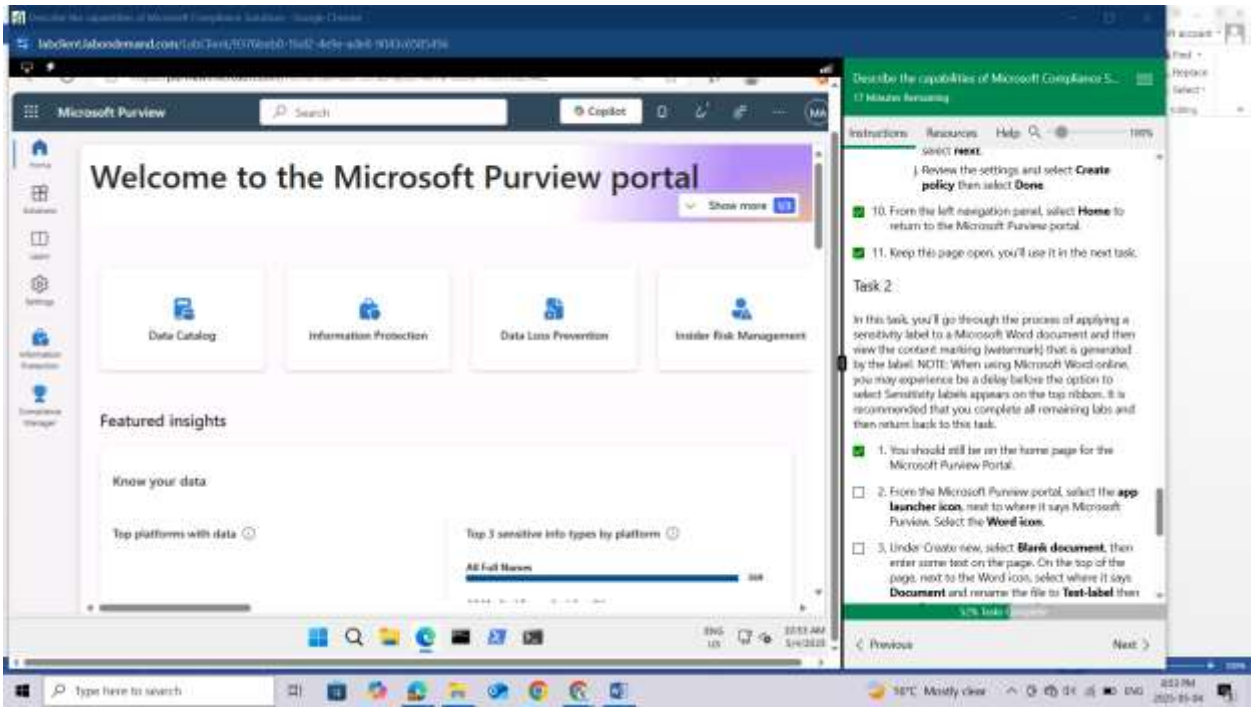

From the left navigation panel, select **Home** to return to the Microsoft Purview portal.

Keep this page open, you'll use it in the next task.

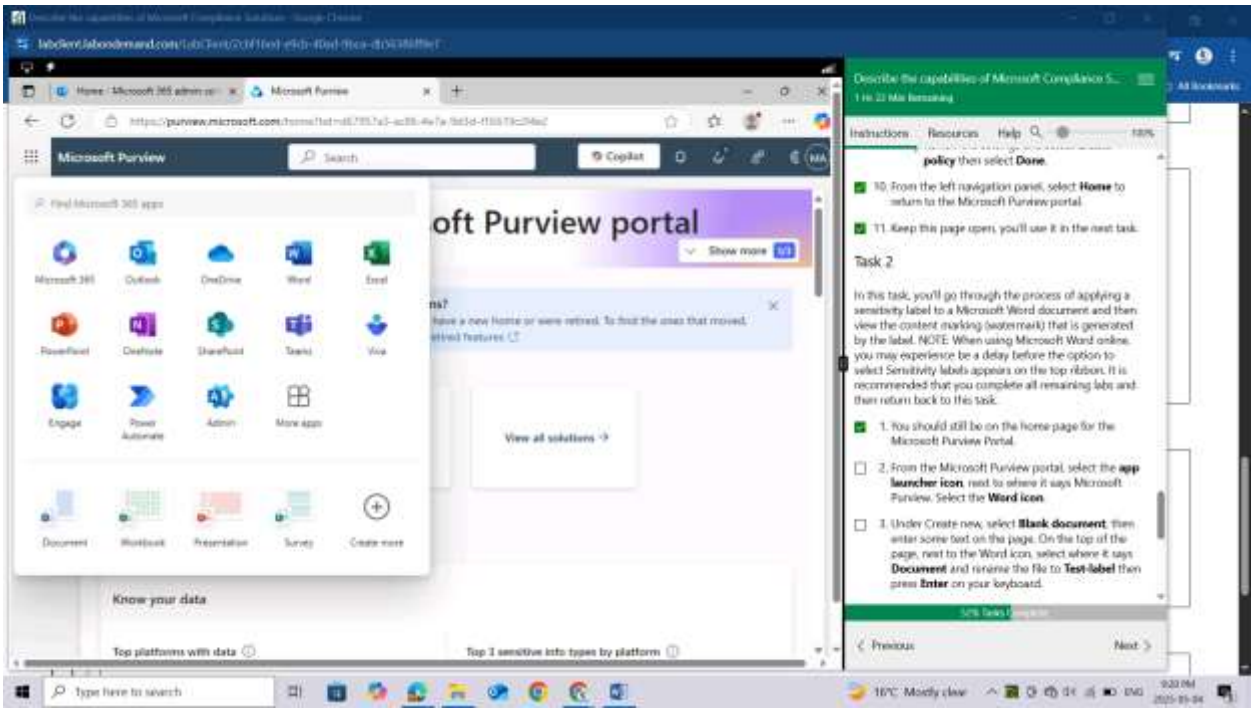
## Task 2

In this task, you'll go through the process of applying a sensitivity label to a Microsoft Word document and then view the content marking (watermark) that is generated by the label. NOTE: When using Microsoft Word online, you may experience be a delay before the option to select Sensitivity labels appears on the top ribbon. It is recommended that you complete all remaining labs and then return back to this task.

You should still be on the home page for the Microsoft Purview Portal.

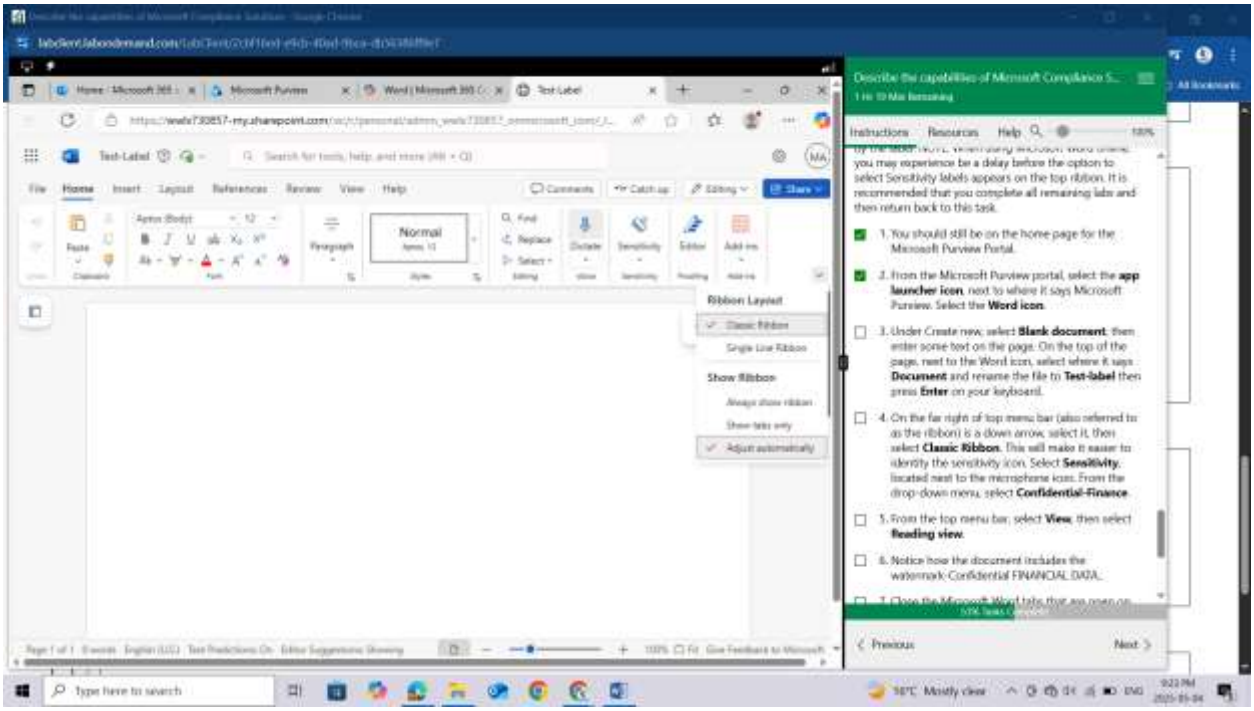



From the Microsoft Purview portal, select the **app launcher icon**, next to where it says Microsoft Purview. Select the **Word icon.**

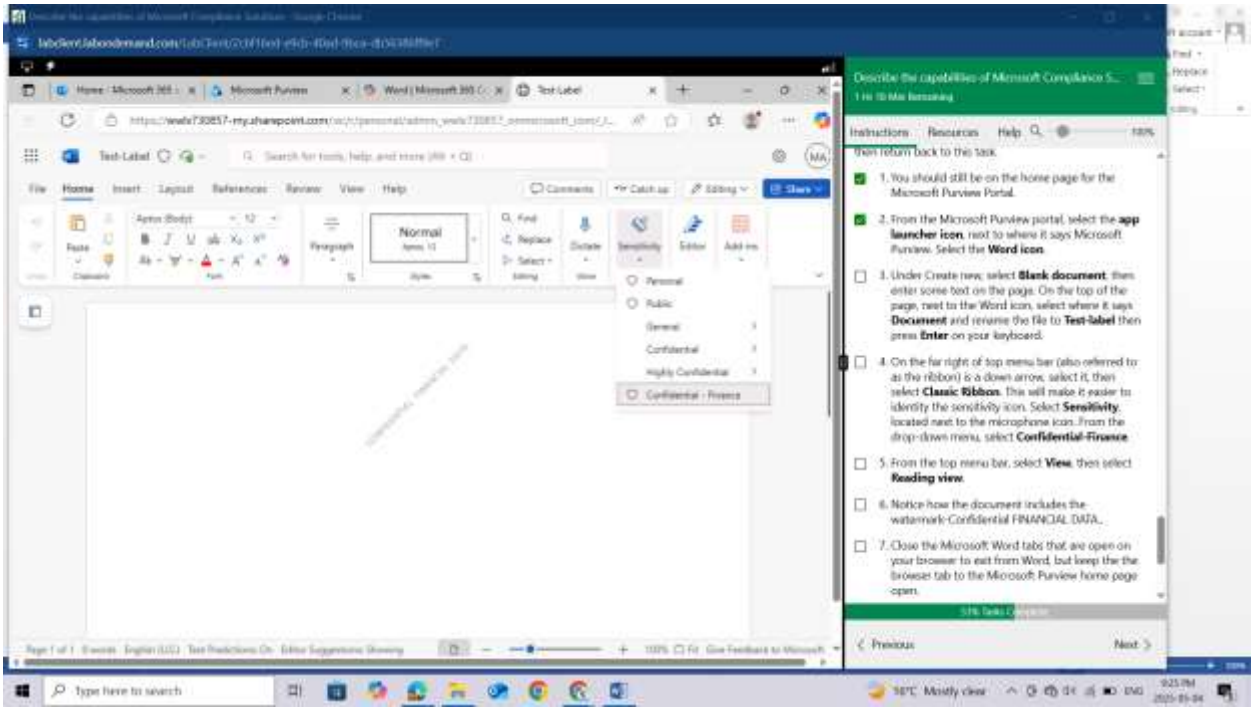



Under Create new, select **Blank document**, then enter some text on the page. On the top of the page, next to the Word icon, select where it says **Document** and rename the file to **Test-label** then press Enter on your keyboard.

On the far right of top menu bar (also referred to as the ribbon) is a down arrow, select it, then select **Classic Ribbon.**

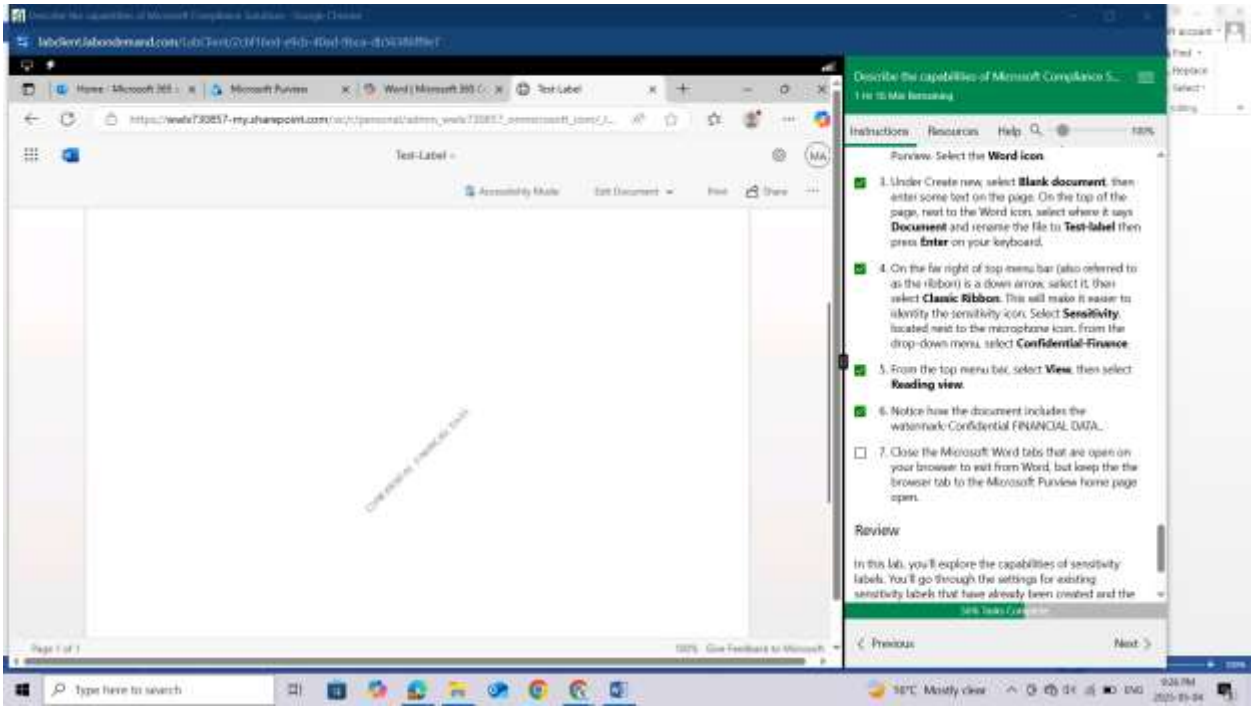


This will make it easier to identity the sensitivity icon. Select **Sensitivity**, located next to the microphone icon. From the drop-down menu, select **Confidential-Finance**.



From the top menu bar, select **View**, then select **Reading view.**

Notice how the document includes the watermark-**Confidential FINANCIAL DATA..**




Close the Microsoft Word tabs that are open on your browser to exit from Word, but keep the browser tab to the Microsoft Purview home page open.

### Review

In this lab, you'll explore the capabilities of sensitivity labels. You'll go through the settings for existing sensitivity labels that have already been created and the corresponding policy to publish the label. Then you'll see how to apply a label.

## 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 events that would need to occur to trigger a policy and the time required are outside of the scope of this exercise.

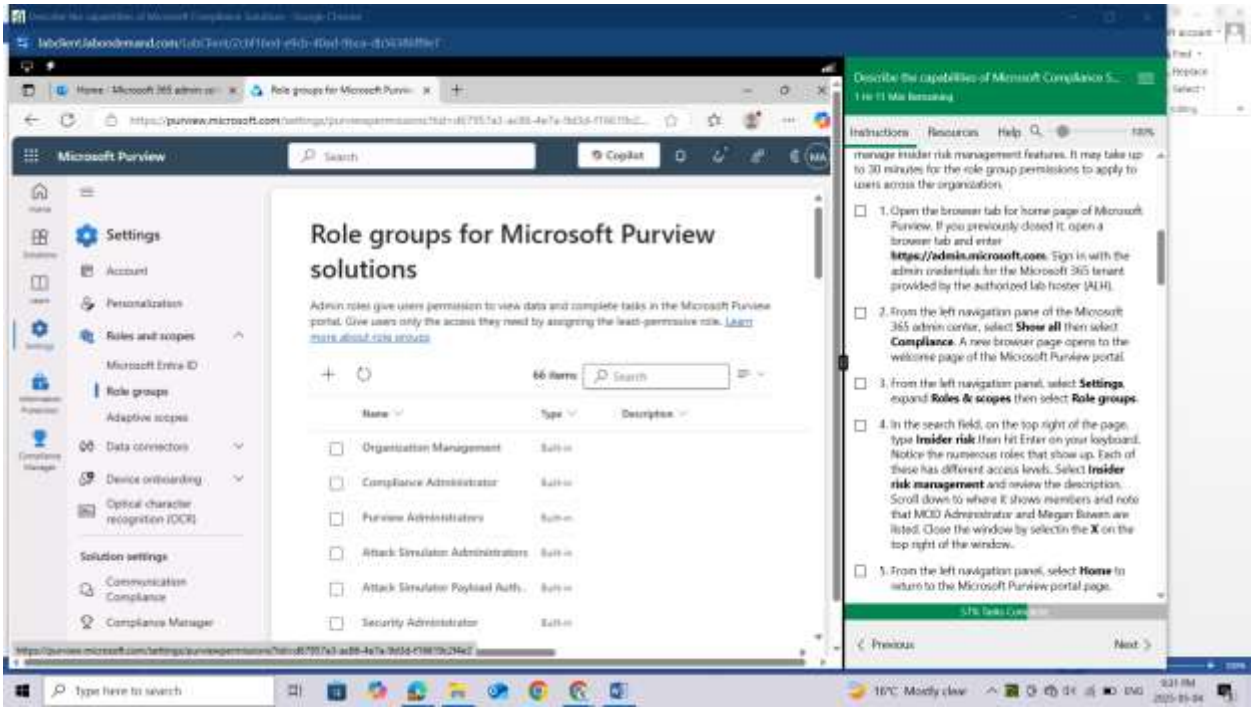
## Task 1

In this task you, as the global administrator, will enable permissions for Insider Risk Management. Specifically, you'll add users to the Insider Risk Management role group to ensure that designated users can access and manage insider risk management features. It may take up to 30 minutes for the role group permissions to apply to users across the organization.

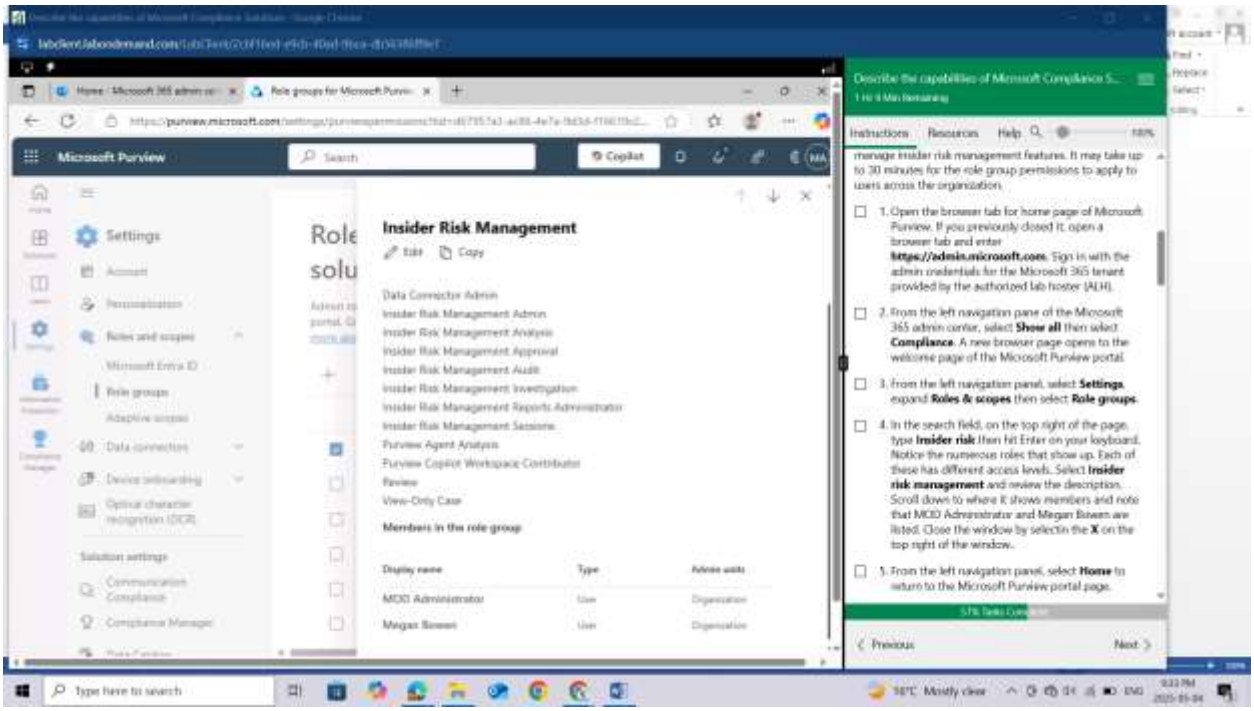
Open the browser tab for home page of Microsoft Purview. If you previously closed it, open a browser tab and enter https://admin.microsoft.com. Sign in with the admin credentials for the Microsoft 365 tenant provided by the authorized lab hoster (ALH).

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.

From the left navigation panel, select **Settings**, expand **Roles & scopes** then select **Role groups.**




In the search field, on the top right of the page, type **Insider risk** then hit Enter on your keyboard. Notice the numerous roles that show up. Each of these has different access levels. Select **Insider risk management** and review the description. Scroll down to where it shows members and note that MOD Administrator and Megan Bowen are listed. Close the window by selectin the X on the top right of the window..




From the left navigation panel, select **Home** to return to the Microsoft Purview portal page.

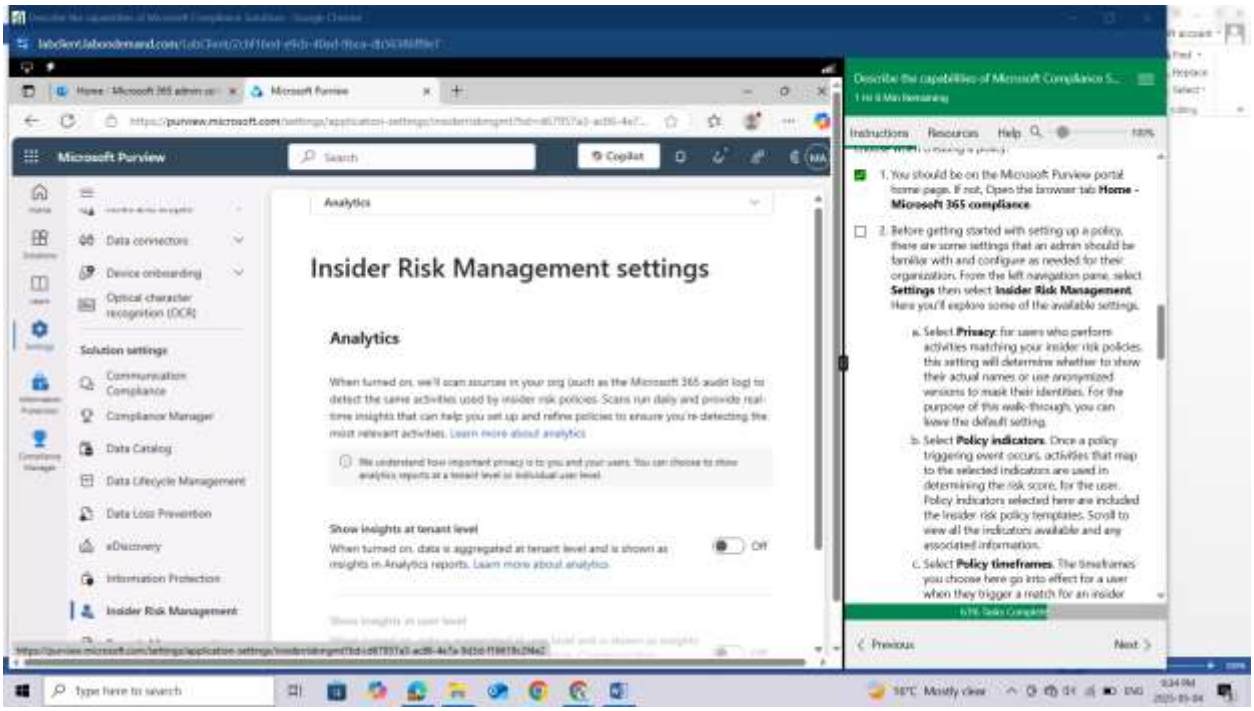
Keep this browser tab open, as you'll come back to it in a subsequent task.

## Task 2

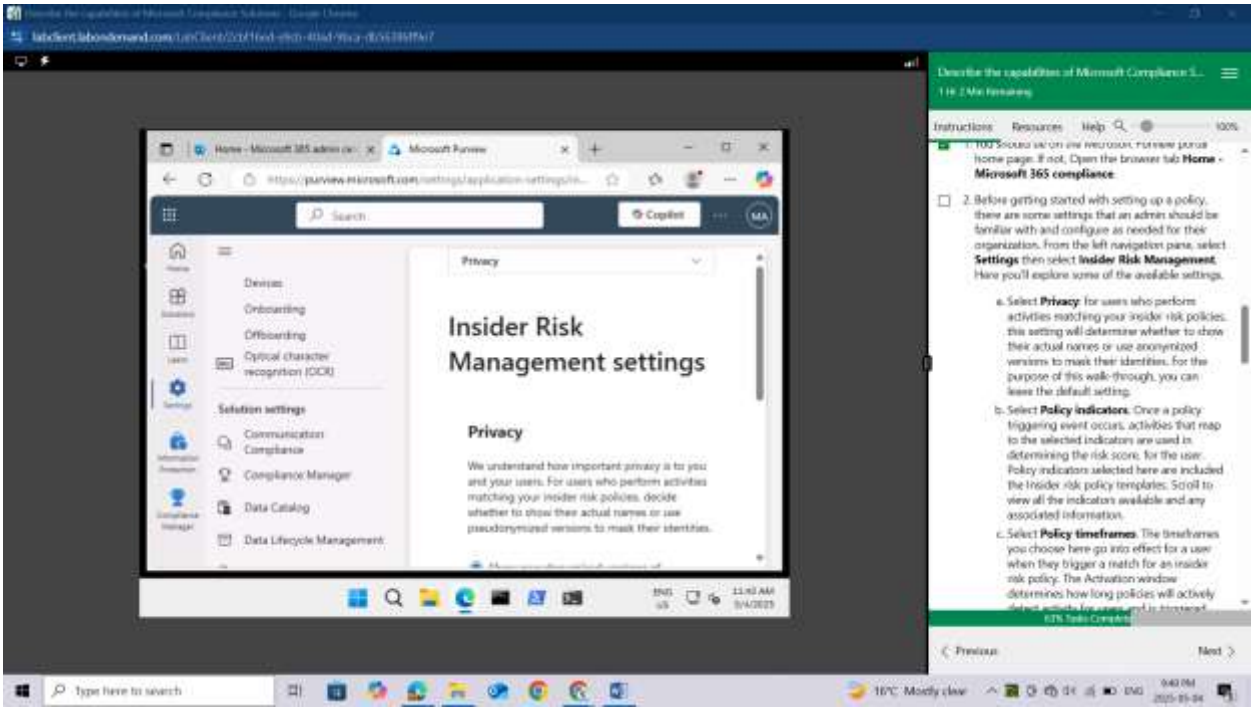
In this task, you'll walk through the settings associated with the Insider Risk Management solution. Insider risk management settings apply to all insider risk management policies, regardless of the template you choose when creating a policy.

You should be on the Microsoft Purview portal home page. If not, Open the browser tab **Home - Microsoft 365 compliance.**

Before getting started with setting up a policy, there are some settings that an admin should be familiar with and configure as needed for their organization. From the left navigation pane, select **Settings** then select **Insider Risk Management.** Here you'll explore some of the available settings.

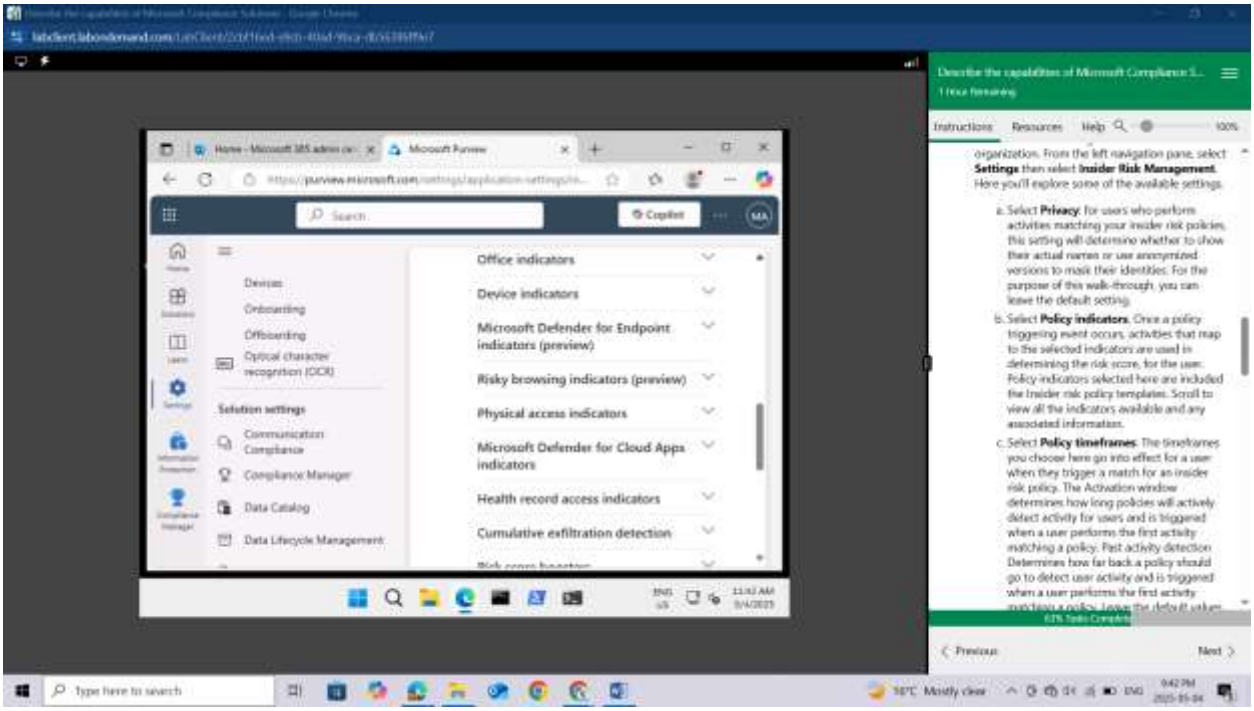



Select **Privacy**: for users who perform activities matching your insider risk policies, this setting will determine whether to show their actual names or use anonymized versions to mask their identities. For the purpose of this walk-through, you can leave the default setting.

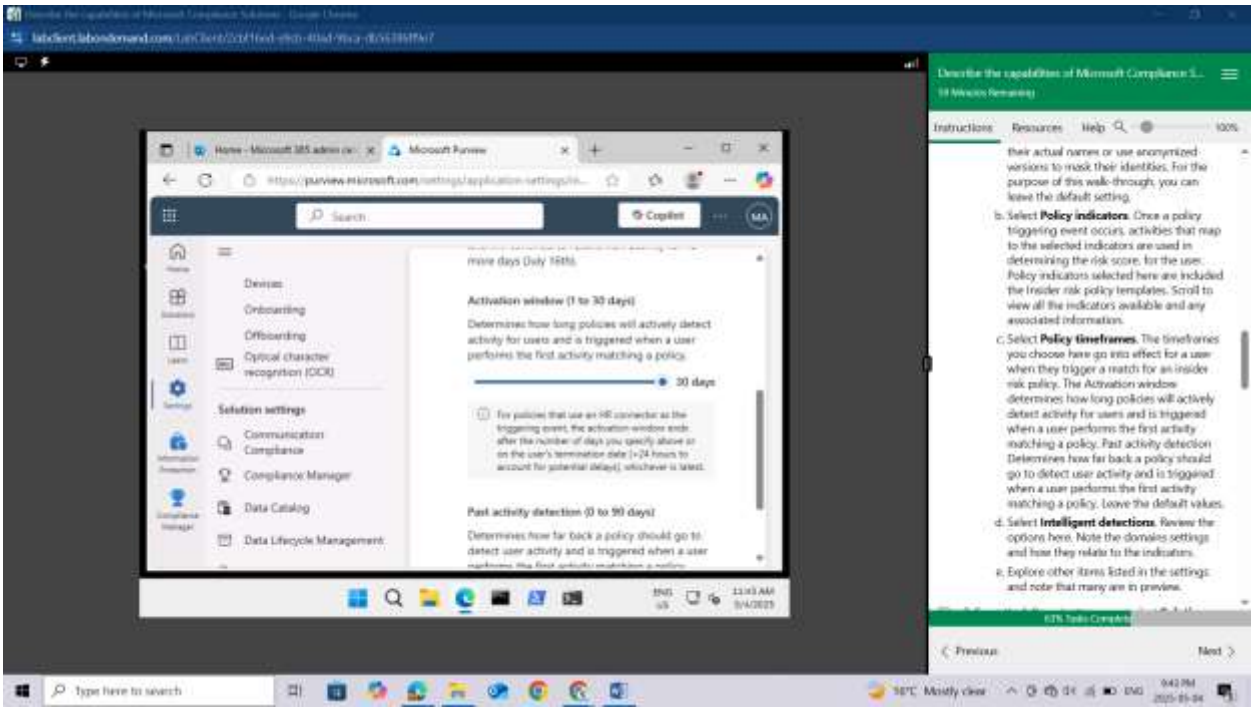



Select **Policy indicators.** Once a policy triggering event occurs, activities that map to the selected indicators are used in determining the risk score, for the user. Policy indicators selected here are

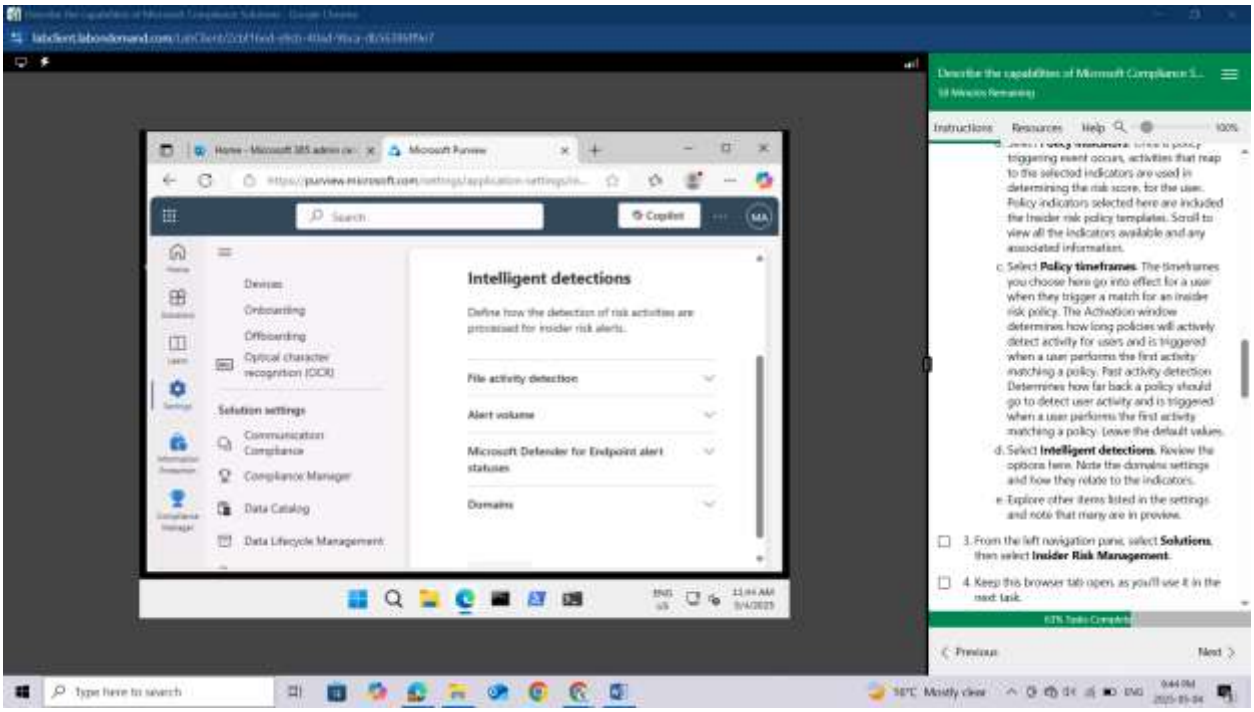
included the Insider risk policy templates. Scroll to view all the indicators available and any associated information.




Select **Policy timeframes.** The timeframes you choose here go into effect for a user when they trigger a match for an insider risk policy. The Activation window determines how long policies will actively detect activity for users and is triggered when a user performs the first activity matching a policy. Past activity detection Determines how far back a policy should go to detect user activity and is triggered when a user performs the first activity matching a policy. Leave the default values.



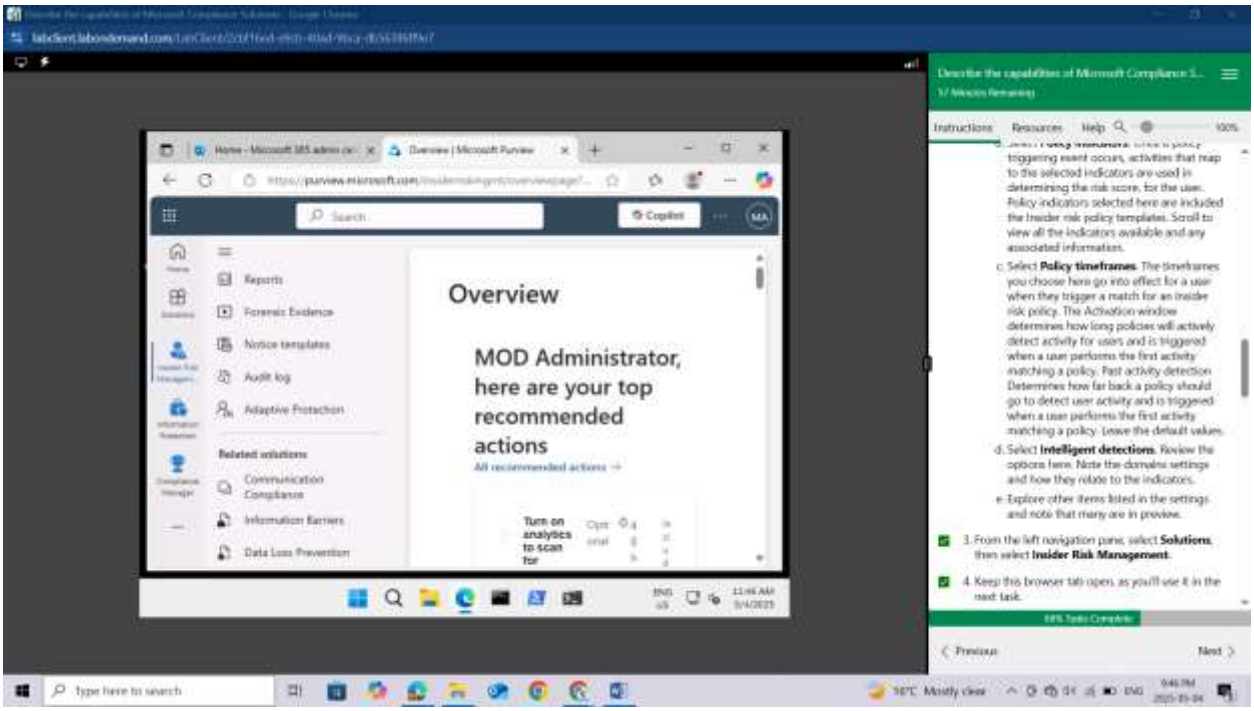
Select **Intelligent detections.** Review the options here. Note the domains settings and how they relate to the indicators.




Explore other items listed in the settings and note that many are in preview.

From the left navigation pane, select **Solutions**, then select **Insider Risk Management.**

Keep this browser tab open, as you'll use it in the next task.

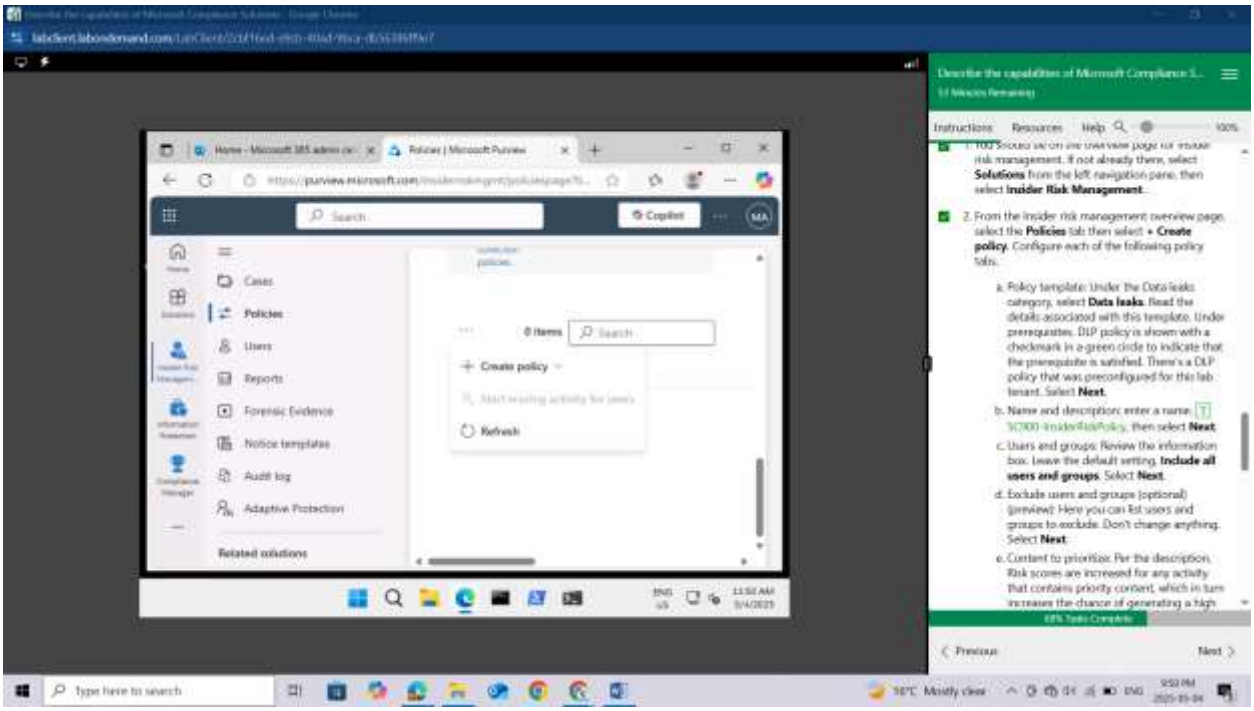



## Task 3

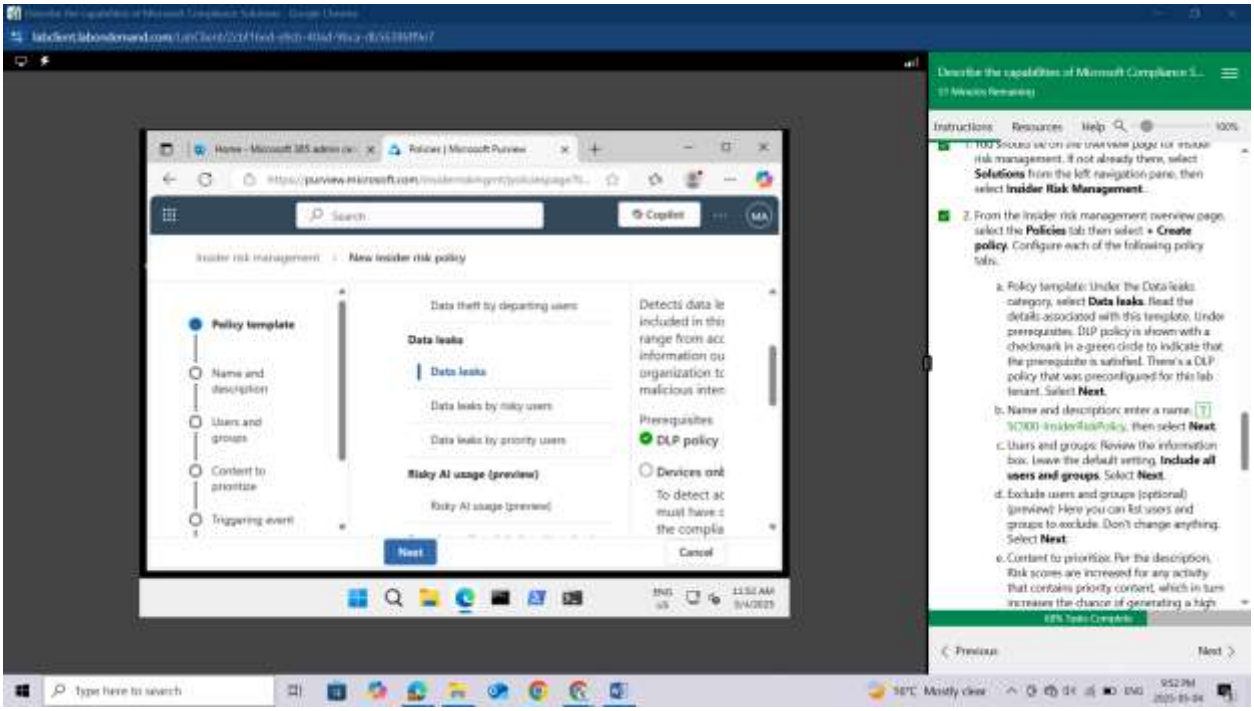
In this task, you'll walk through the settings for creating a policy. The objective is simply to get a sense of the various options and flexibility associated with creating a policy.

You should be on the overview page for **Insider risk management**. If not already there, select **Solutions** from the left navigation pane, then select **Insider Risk Management.**

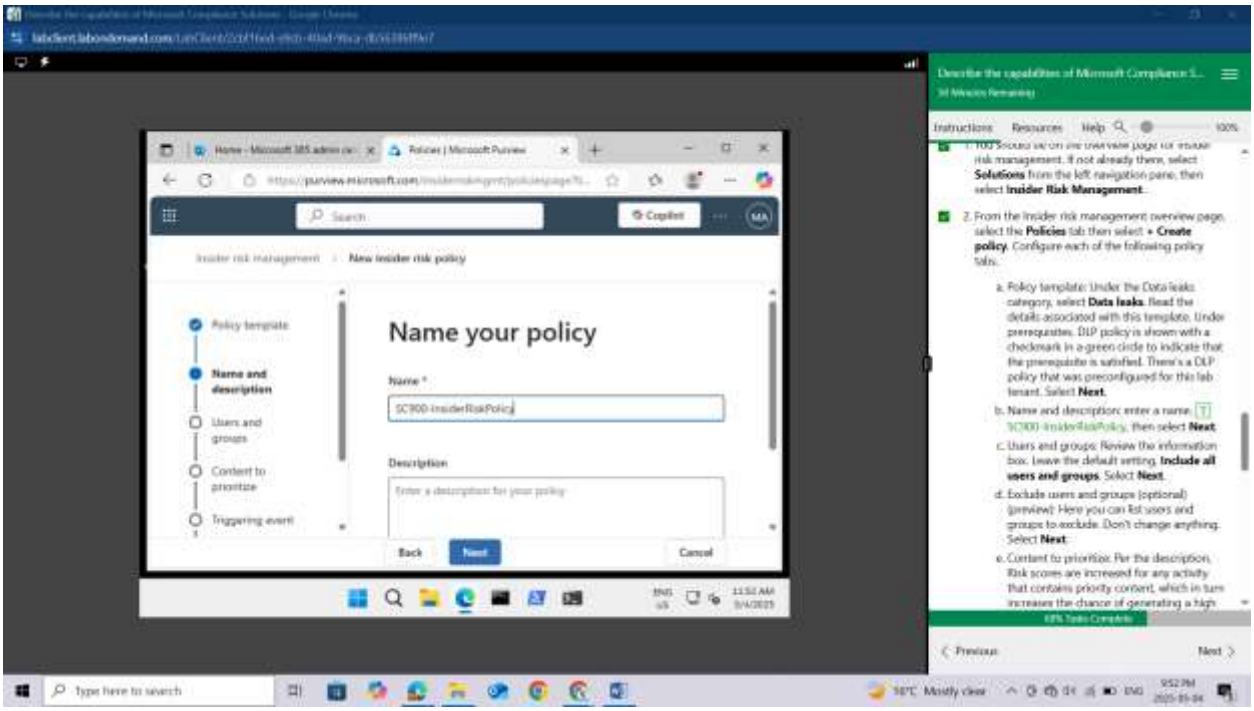
From the Insider risk management overview page, select the **Policies** tab then select **+ Create policy.** Configure each of the following policy tabs.



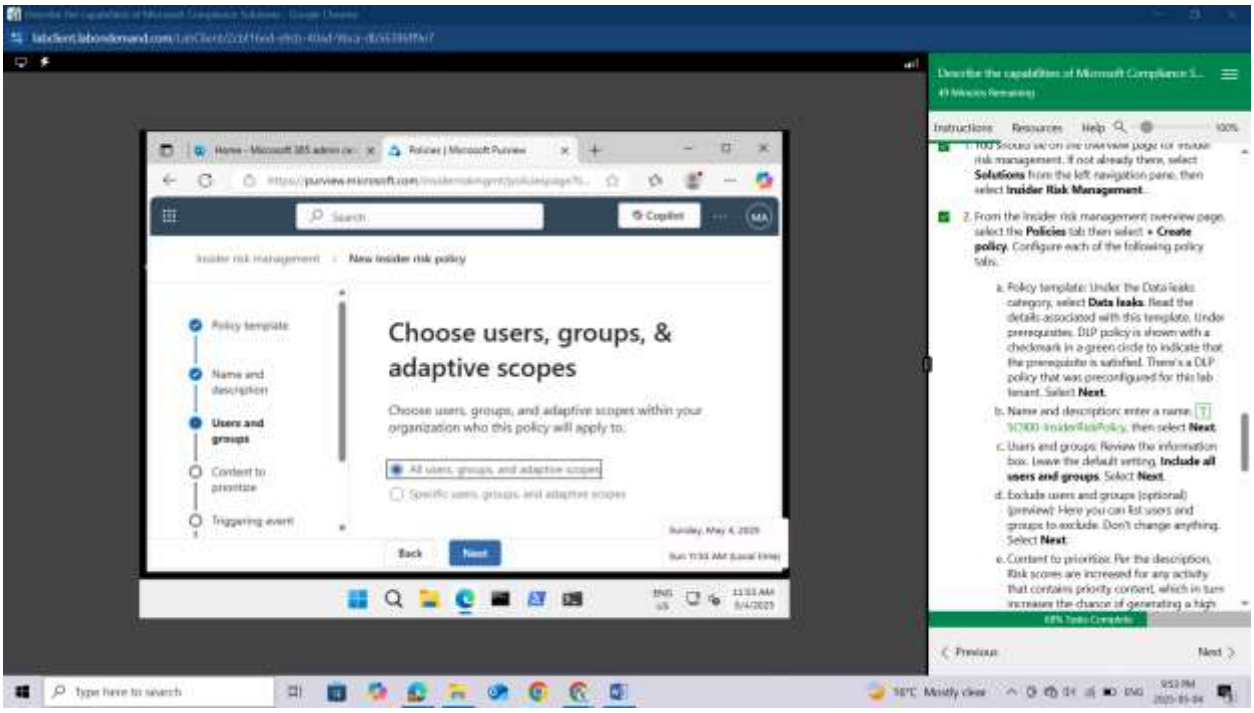

**Policy template:** Under the Data leaks category, select Data leaks. Read the details associated with this template. Under prerequisites, DLP policy is shown with a checkmark in a green circle to indicate that the prerequisite is satisfied. There's a DLP policy that was preconfigured for this lab tenant. Select **Next**.



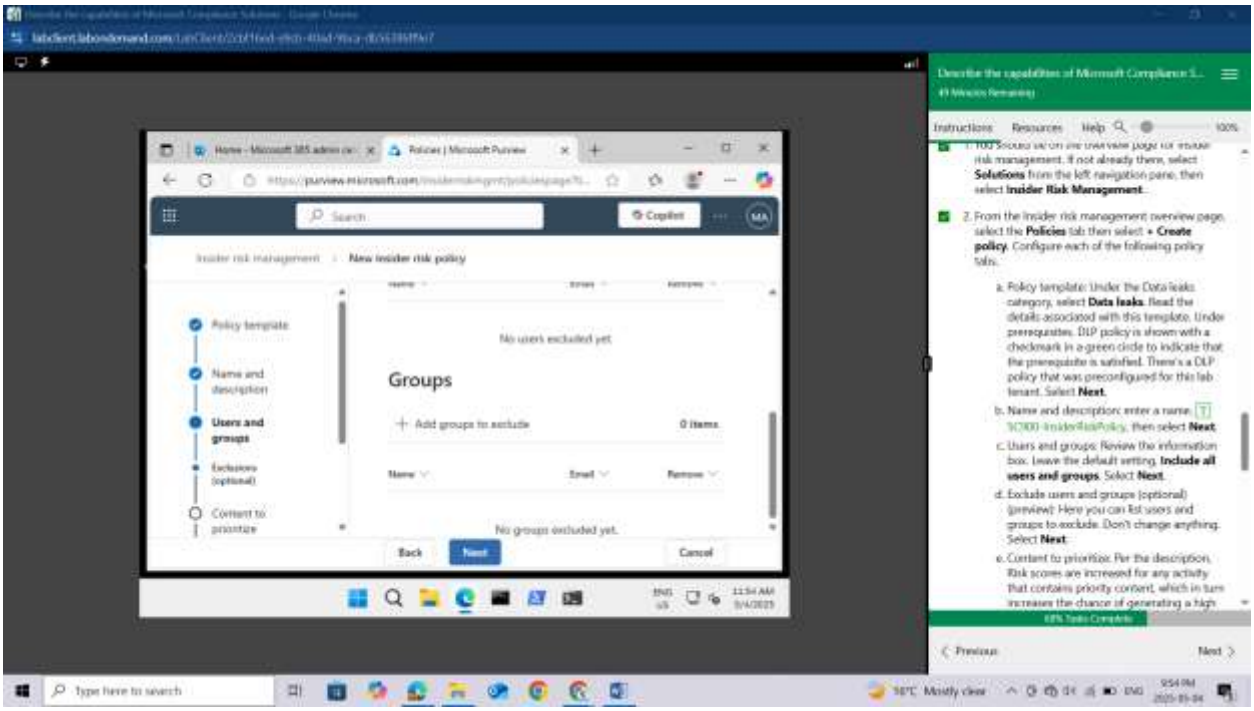

**Name and description:** enter a name, SC900-InsiderRiskPolicy, then select **Next**.



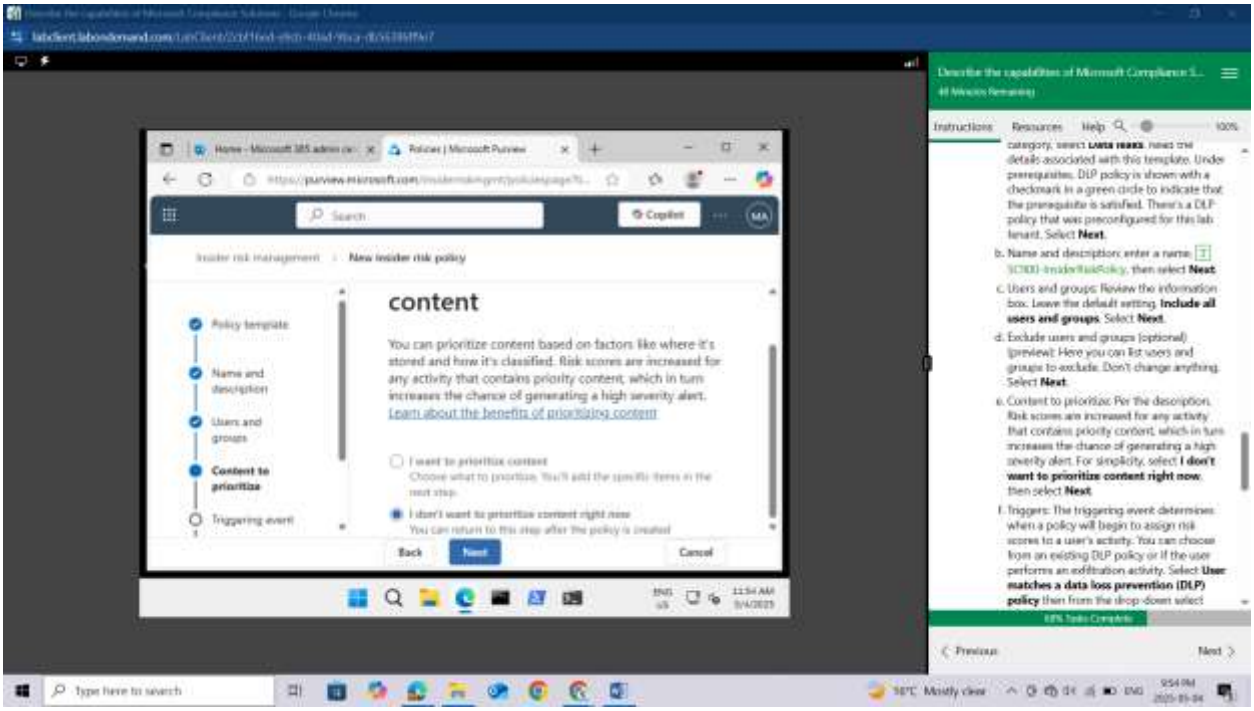

**Users and groups:** Review the information box. Leave the default setting, Include all users and groups. Select **Next**.




**Exclude users and groups (optional)(preview):** Here you can list users and groups to exclude. Don't change anything. Select **Next**.

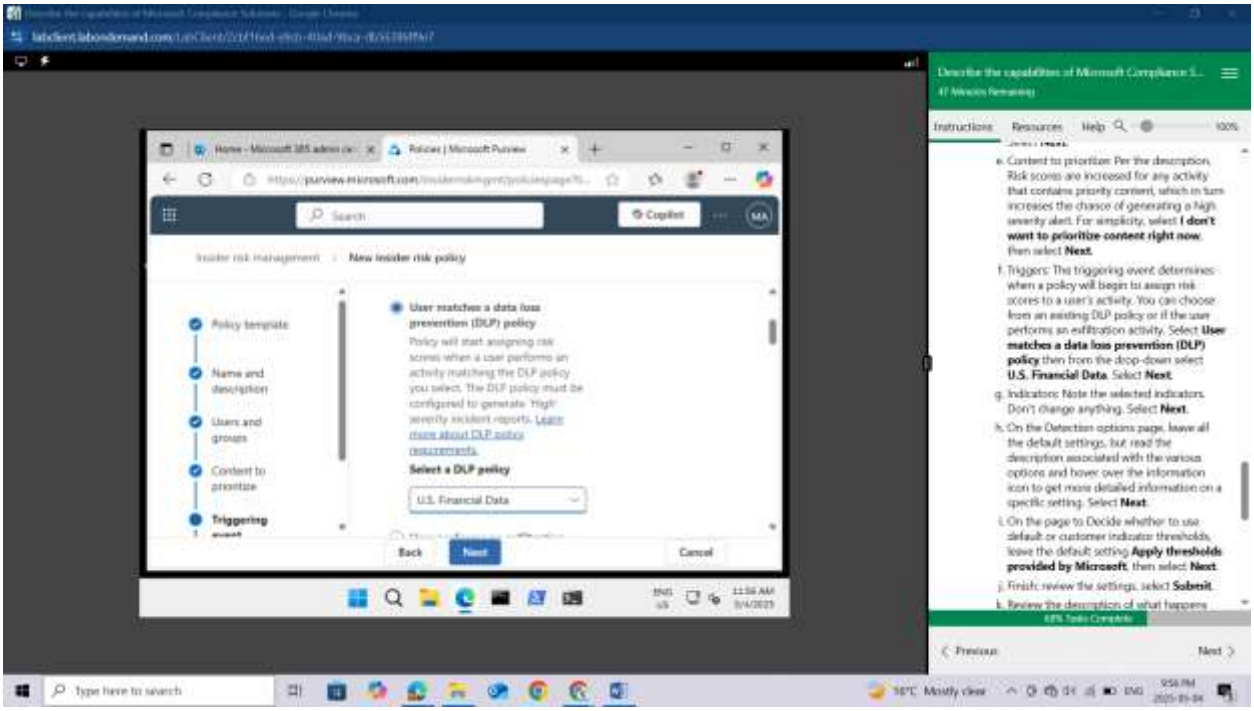



**Content to prioritize:** Per the description, Risk scores are increased for any activity that contains priority content, which in turn increases the chance of generating a high severity alert. For simplicity, select **I don't want to prioritize content right now**, then select **Next**.

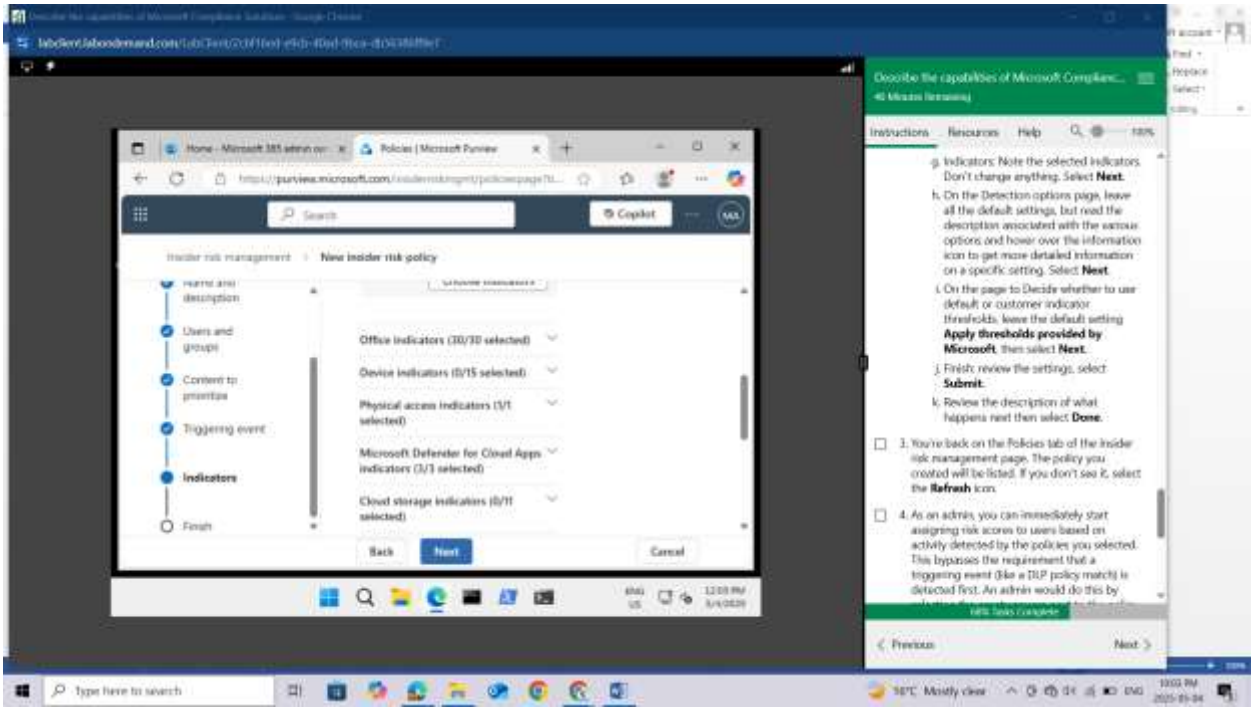



**Triggers**: The triggering event determines when a policy will begin to assign risk scores to a user's activity. You can choose from an existing DLP policy or if the user performs an exfiltration activity. Select

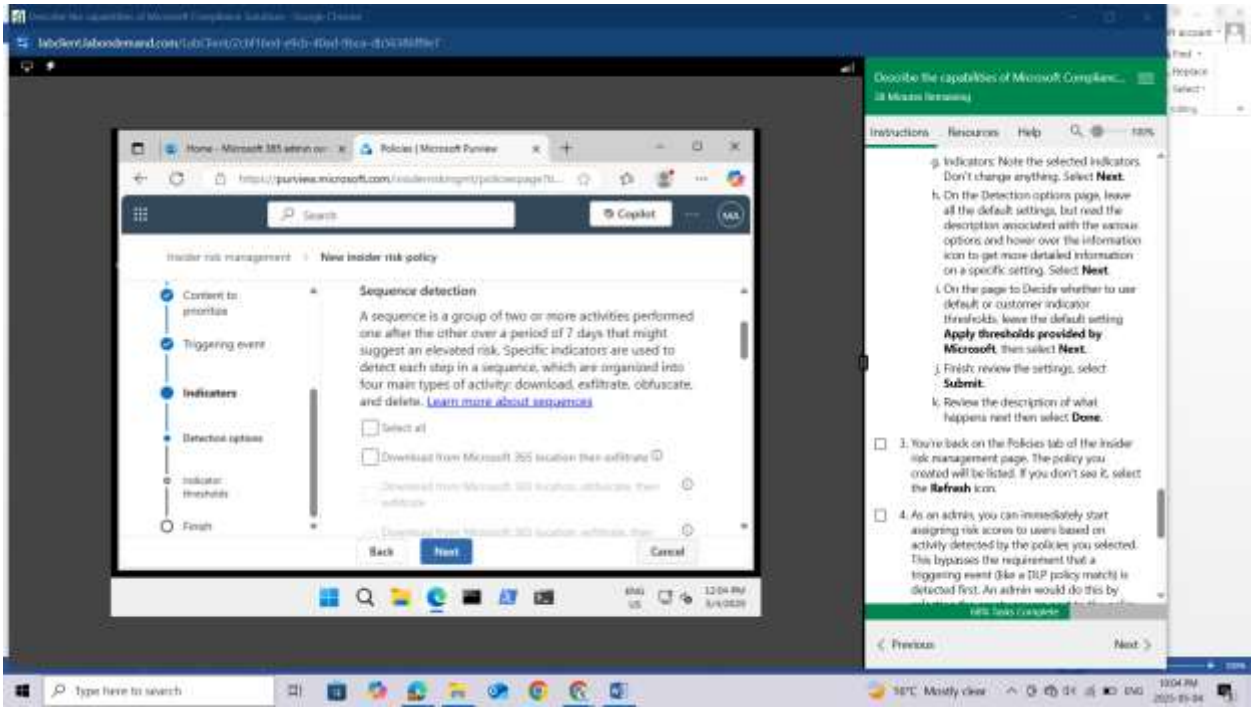
**User matches a data loss prevention (DLP) policy** then from the drop-down select **U.S. Financial Data.** Select **Next**.



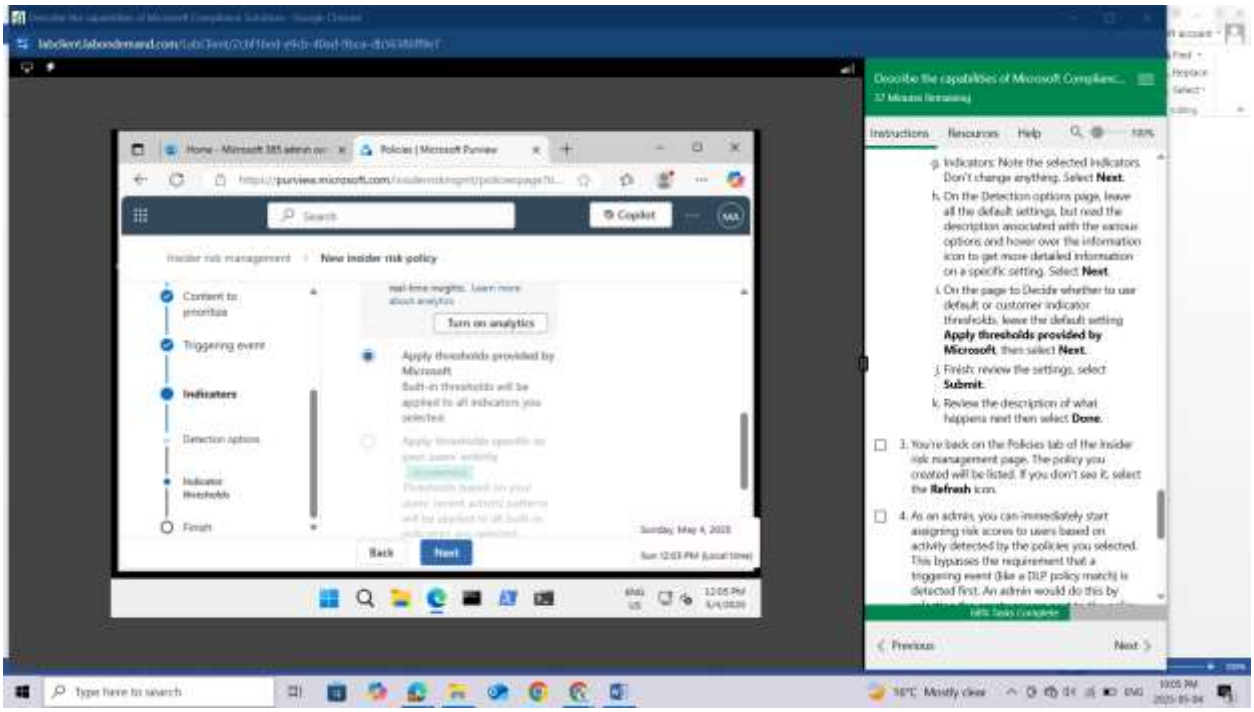

**Indicators:** Note the selected indicators, But to know the selected indicators I turned ON. Don't change anything. Select **Next**.



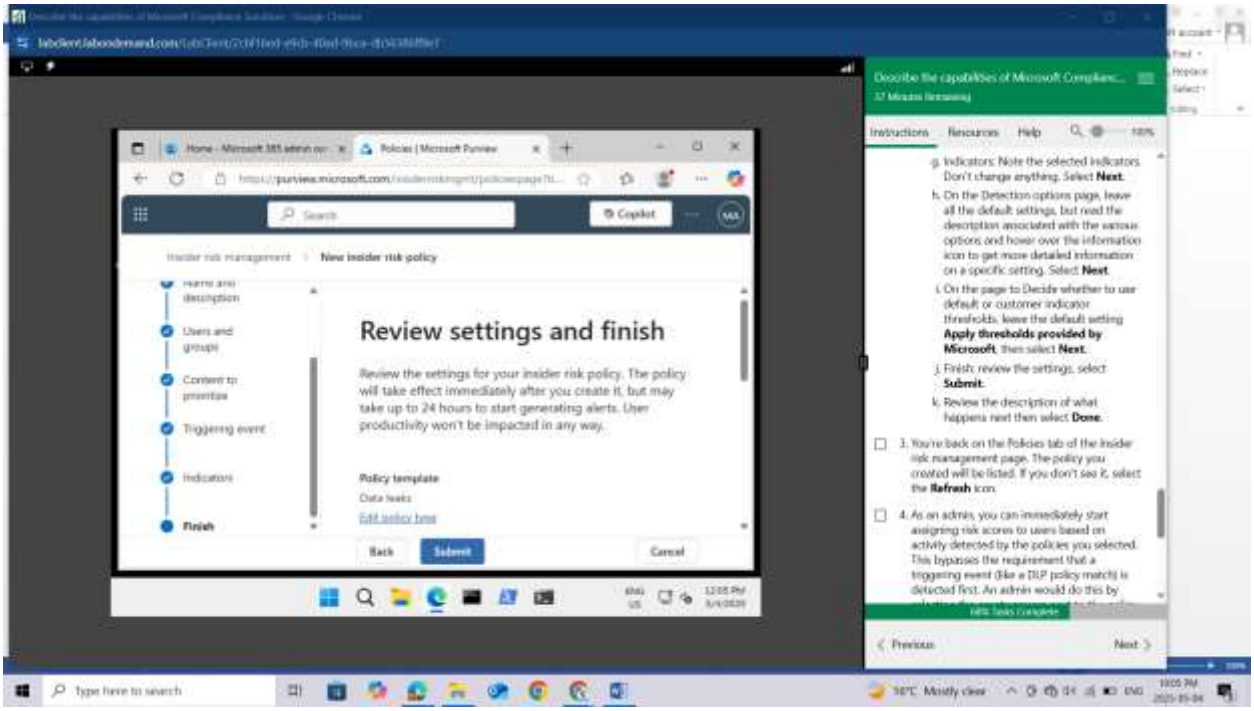
On the Detection options page, leave all the default settings, but read the description associated with the various options and hover over the information icon to get more detailed information on a specific setting. Select **Next**.



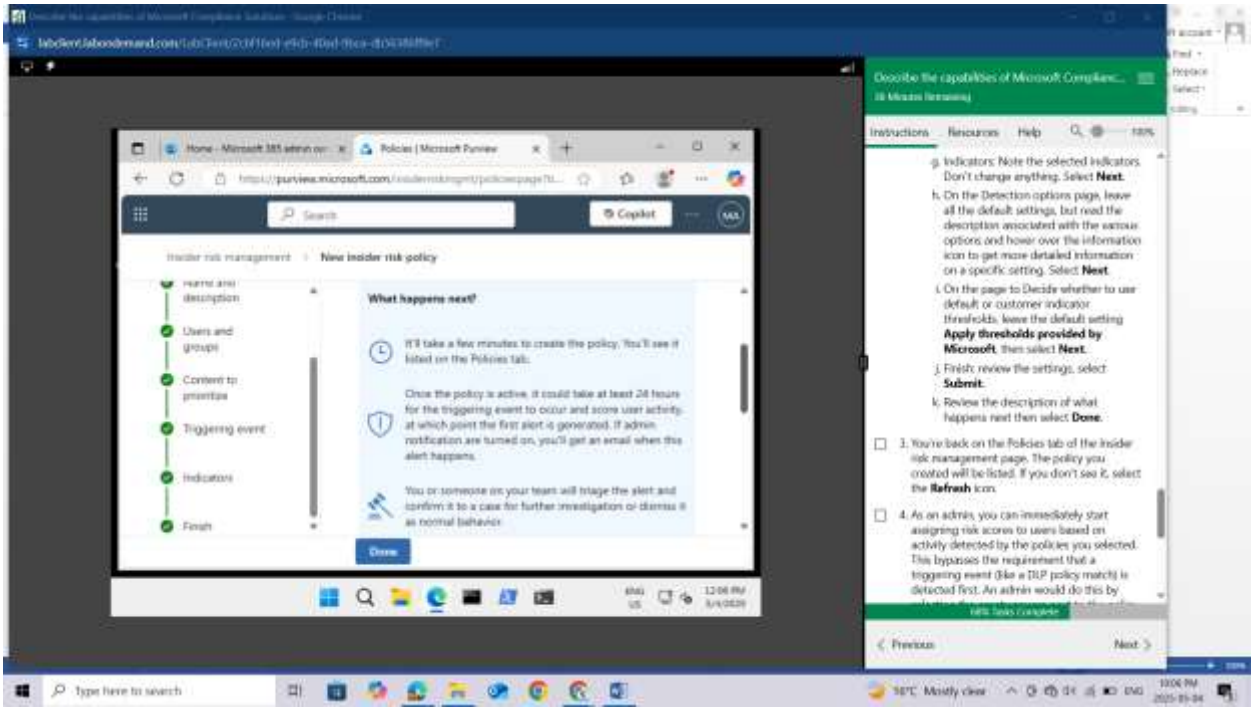

On the page to Decide whether to use default or customer indicator thresholds, leave the default setting Apply thresholds provided by Microsoft, then select **Next**.



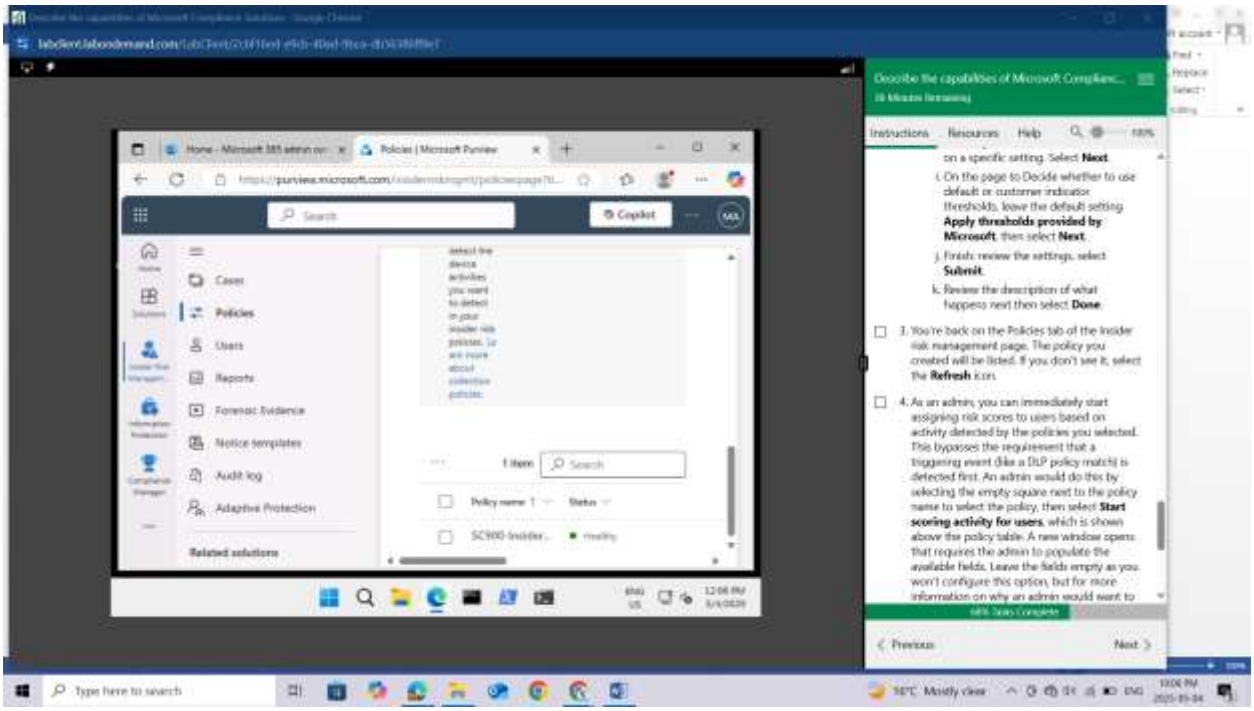
**Finish**: review the settings, select **Submit**.



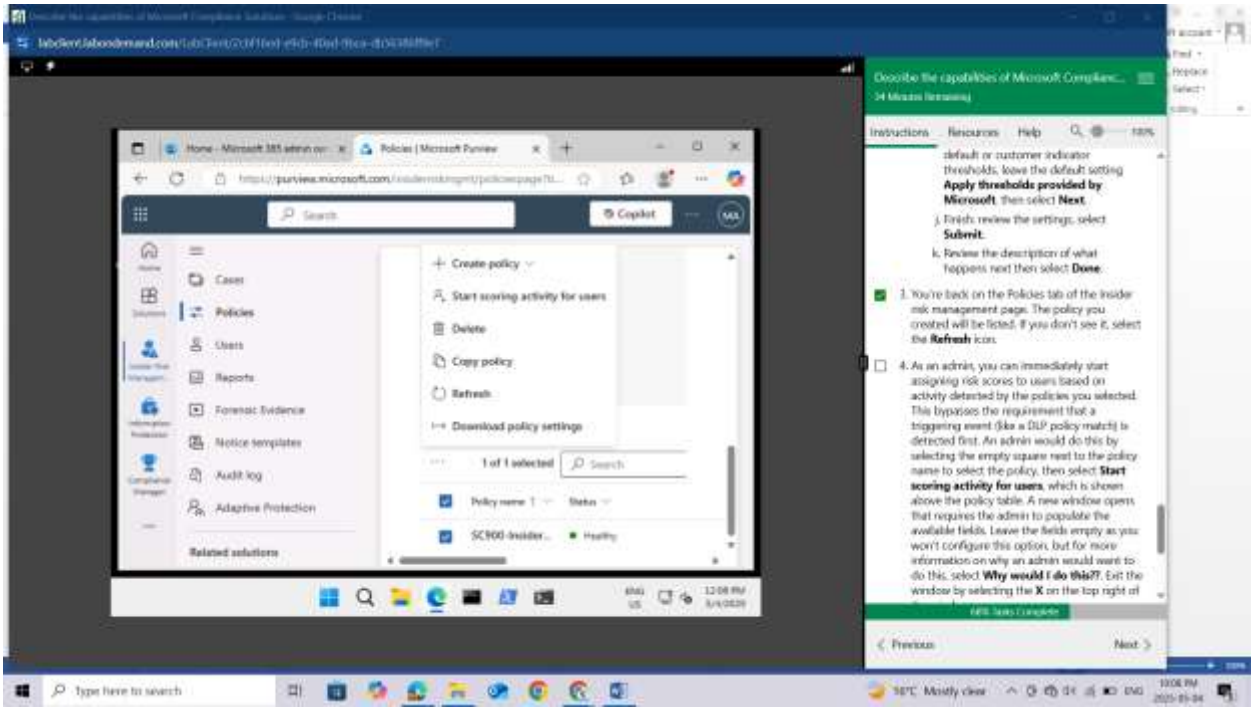

Review the description of what happens next then select **Done**.




You're back on the Policies tab of the Insider risk management page. The policy you created will be listed. If you don't see it, select the **Refresh** icon.

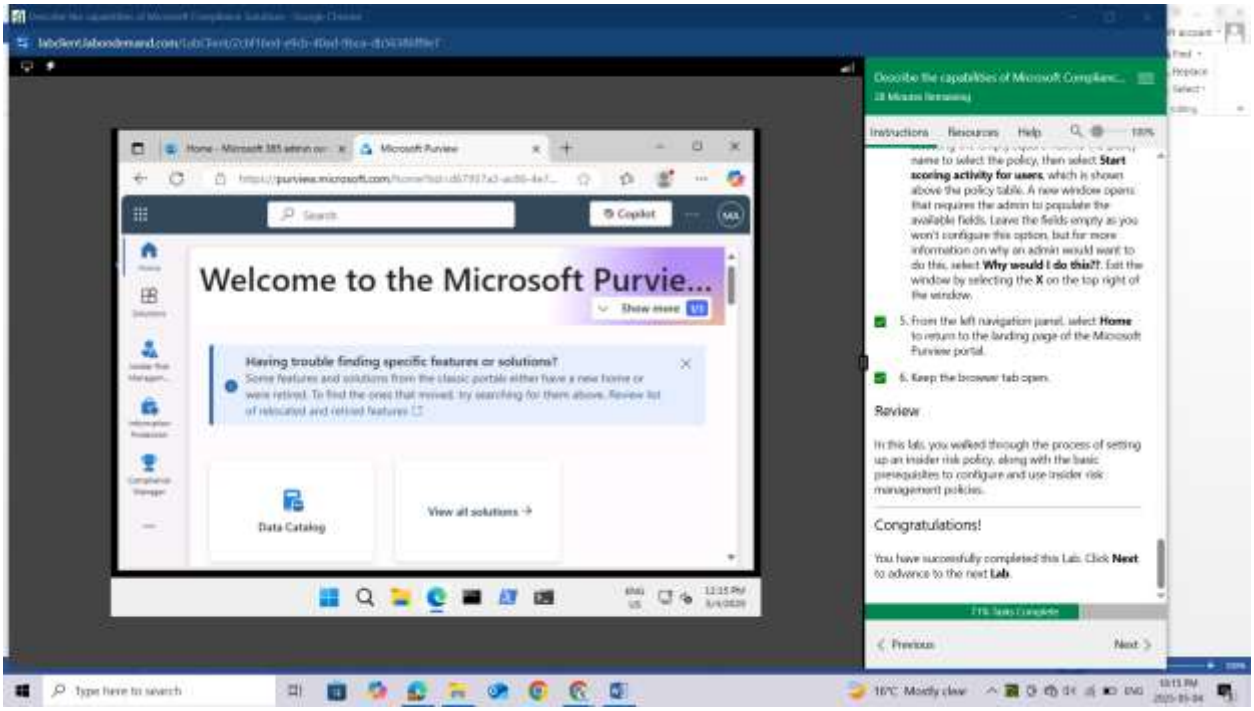


As an admin, you can immediately start assigning risk scores to users based on activity detected by the policies you selected. This bypasses the requirement that a triggering event (like a DLP policy match) is detected first. An admin would do this by selecting the empty square next to the policy name to select the policy, then select Start scoring activity for users, which is shown above the policy table. A new window opens that requires the admin to populate the available fields. Leave the fields empty as you won't configure this option, but for more information on why an admin would want to do this, select Why would I do this??. Exit the window by selecting the X on the top right of the window.



From the left navigation panel, select **Home** to return to the landing page of the Microsoft Purview portal.

Keep the browser tab open.




# LAB: EXPLORE EDISCOVERY

This lab maps to the following Learn content:

Learning Path: Describe the capabilities of Microsoft Priva and Microsoft Purview

Module: Describe the data compliance solutions of Microsoft Purview

Unit: Describe eDiscovery

## Lab scenario

In this lab you'll go through the steps required for setting up eDiscovery, including setting up role permissions, creating an eDiscovery case, creating an eDiscovery hold and creating a search query. Note: Licensing for eDiscovery (Standard) requires the appropriate organization subscription and per-user licensing. If you aren't sure which licenses support eDiscovery (Standard), visit Get started with eDiscovery (Standard) in Microsoft Purview.

## Task 1

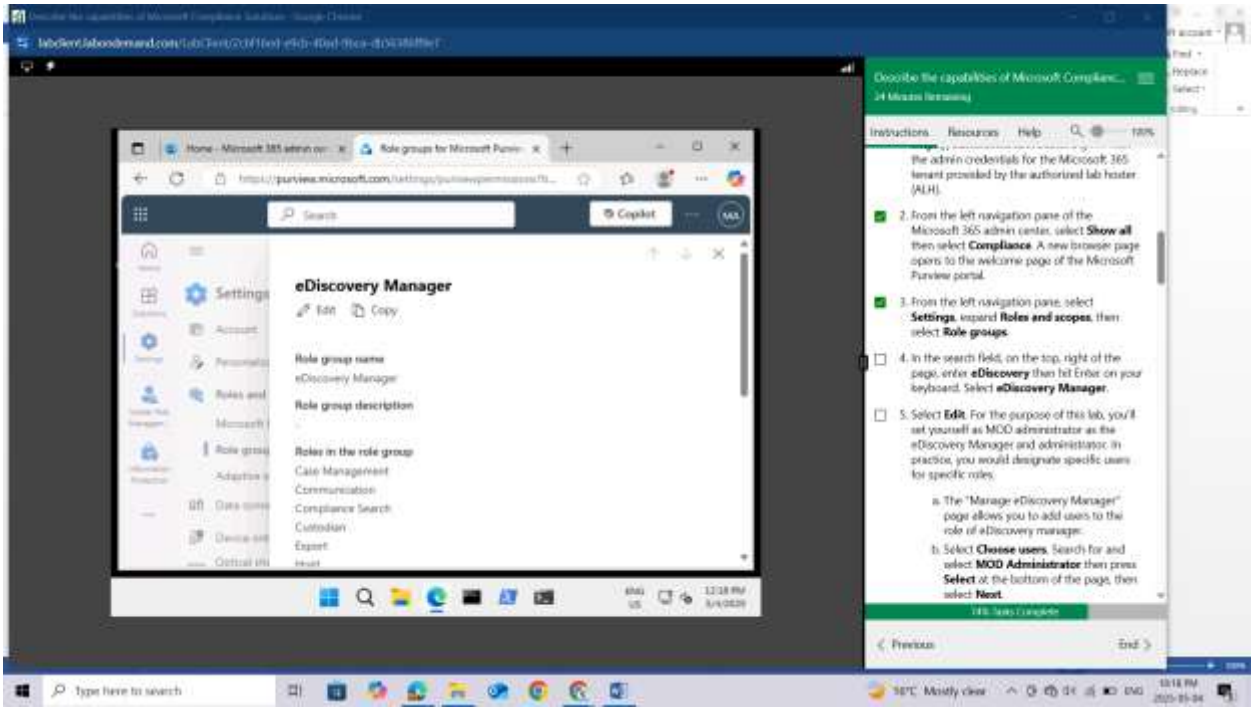
To access eDiscovery (Standard) or be added as a member of an eDiscovery case, a user must be assigned the appropriate permissions. In this task, you as the global admin, will add specific users as members of the eDiscovery Manager role group.

Open the browser tab for home page of Microsoft Purview. If you previously closed it, open a browser tab and enter https://admin.microsoft.com. Sign in with the admin credentials for the Microsoft 365 tenant provided by the authorized lab hoster (ALH).

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.

From the left navigation pane, select **Settings**, expand **Roles and scopes**, then select **Role groups**.

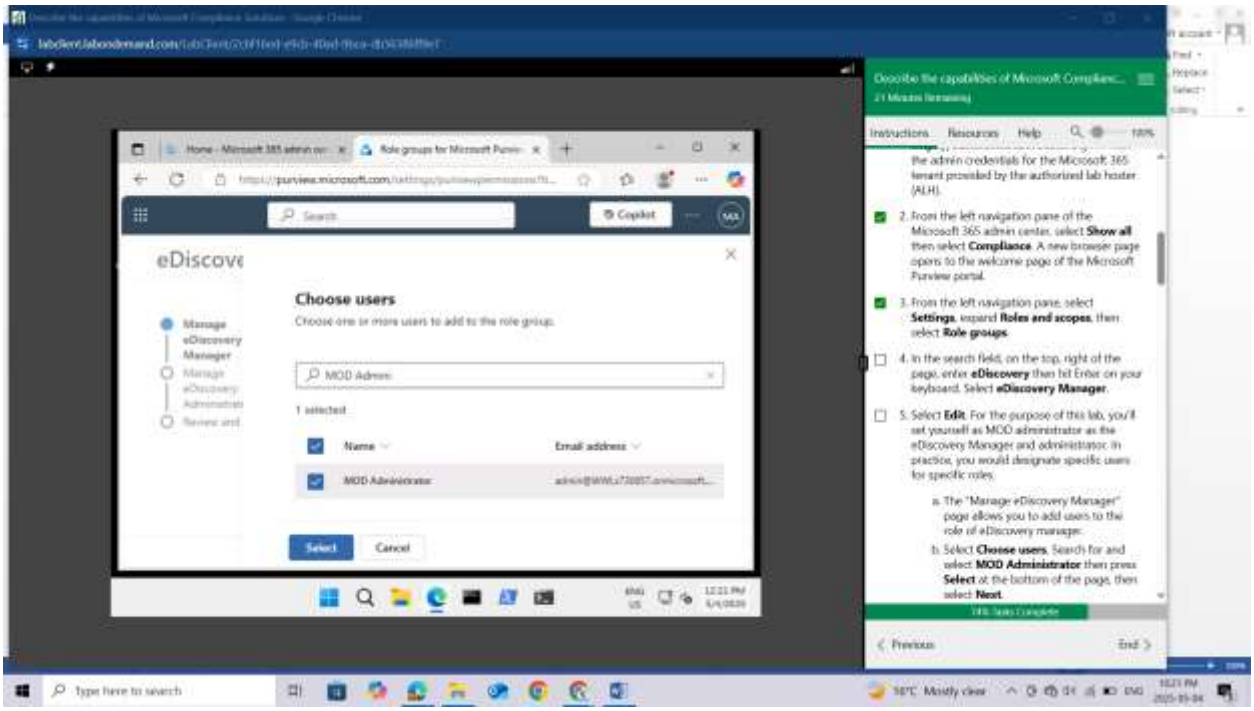
In the search field, on the top, right of the page, enter **eDiscovery** then hit Enter on your keyboard. Select **eDiscovery Manager**.



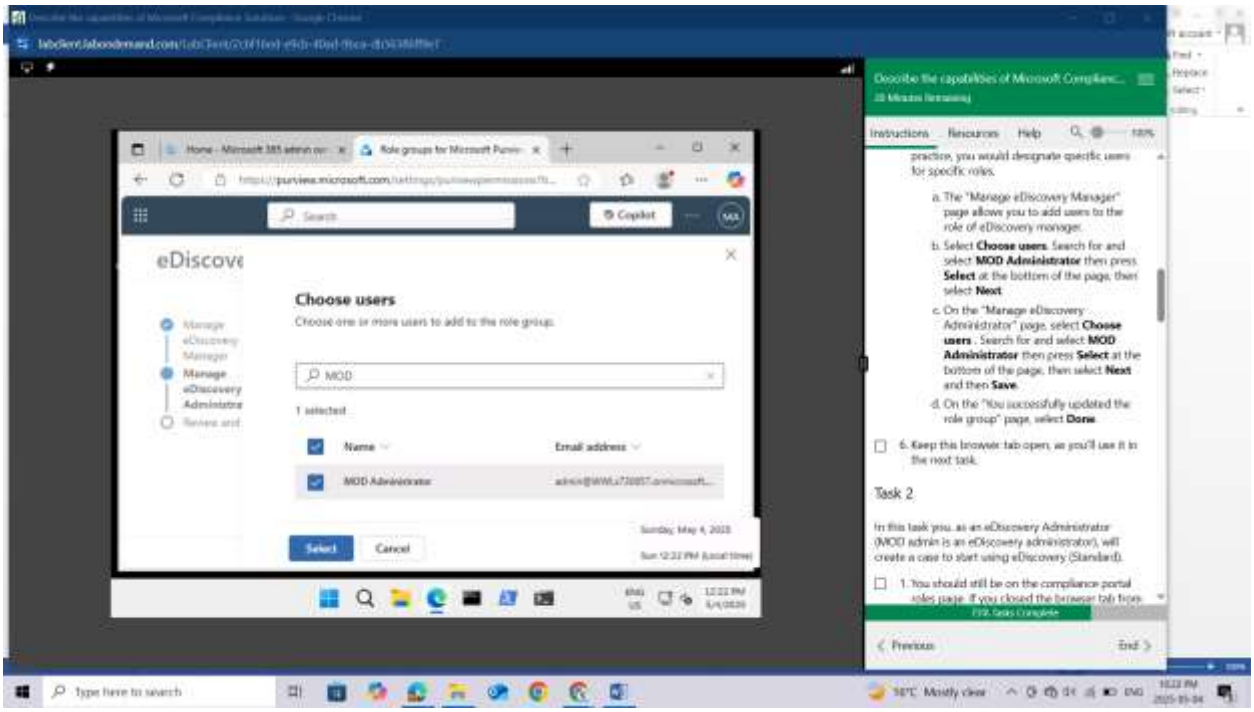

Select **Edit**. For the purpose of this lab, you'll set yourself as MOD administrator as the eDiscovery Manager and administrator. In practice, you would designate specific users for specific roles.

The "Manage eDiscovery Manager" page allows you to add users to the role of eDiscovery manager.

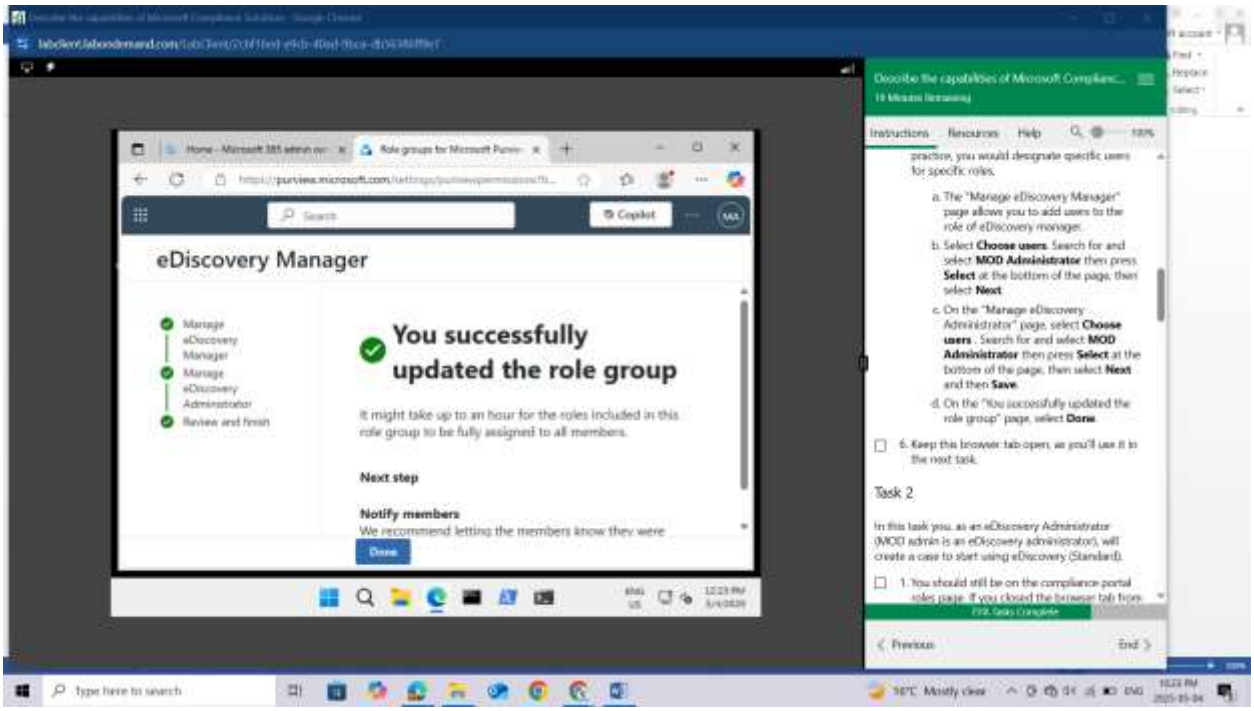
Select **Choose users**. Search for and select **MOD Administrator** then press **Select** at the bottom of the page, then select **Next**.




On the "Manage eDiscovery Administrator" page, select **Choose users**. Search for and select **MOD Administrator** then press **Select** at the bottom of the page, then select **Next** and then **Save**.




On the "You successfully updated the role group" page, select **Done**.



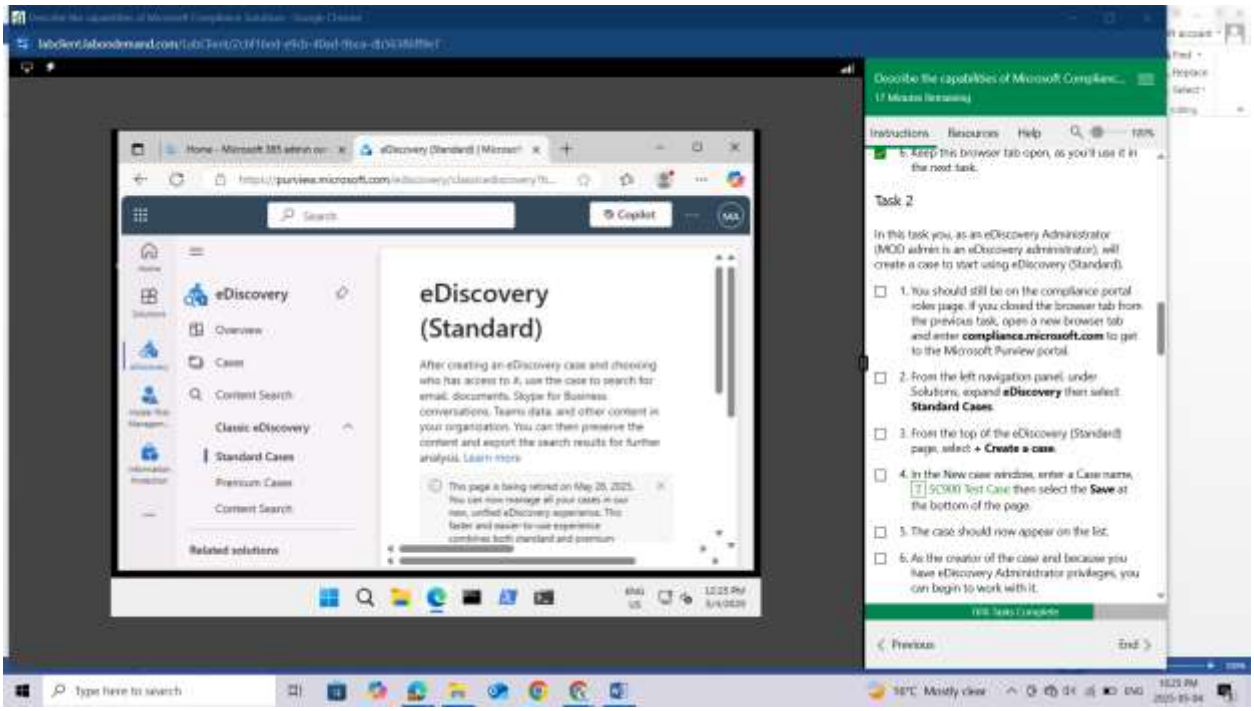

Keep this browser tab open, as you'll use it in the next task.

## Task 2

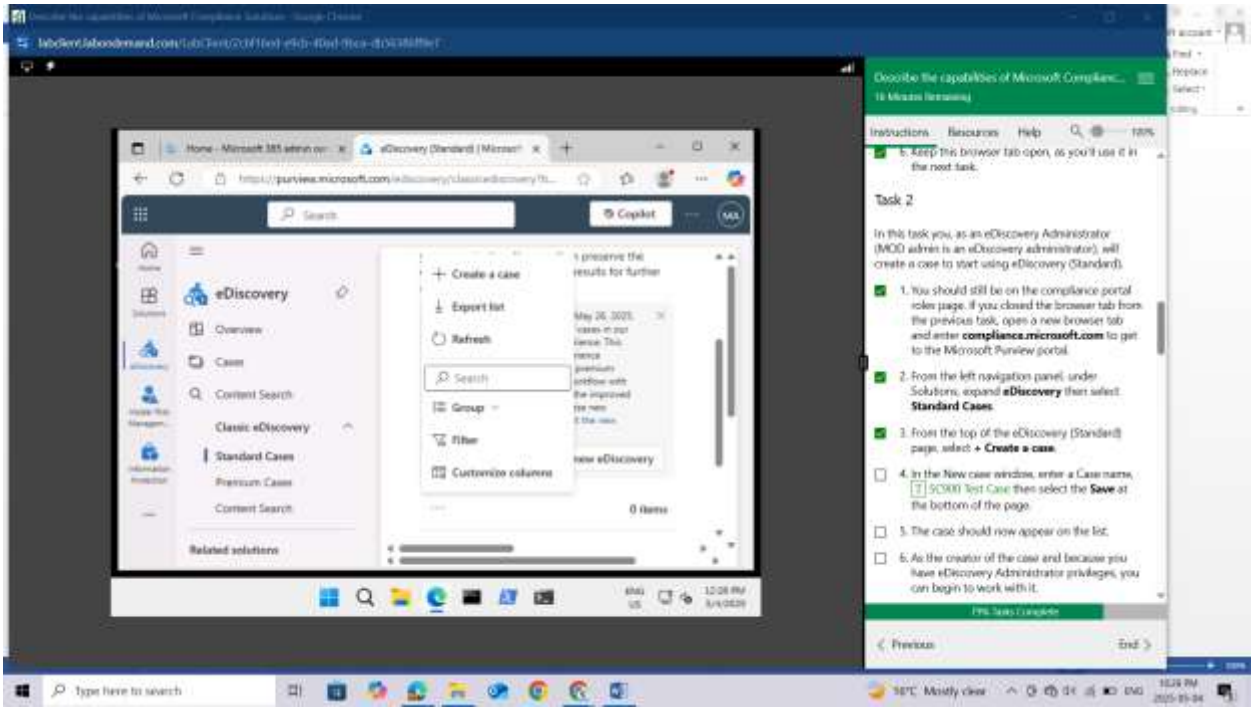
In this task you, as an eDiscovery Administrator (MOD admin is an eDiscovery administrator), will create a case to start using eDiscovery (Standard).

You should still be on the compliance portal roles page. If you closed the browser tab from the previous task, open a new browser tab and enter compliance.microsoft.com to get to the Microsoft Purview portal.

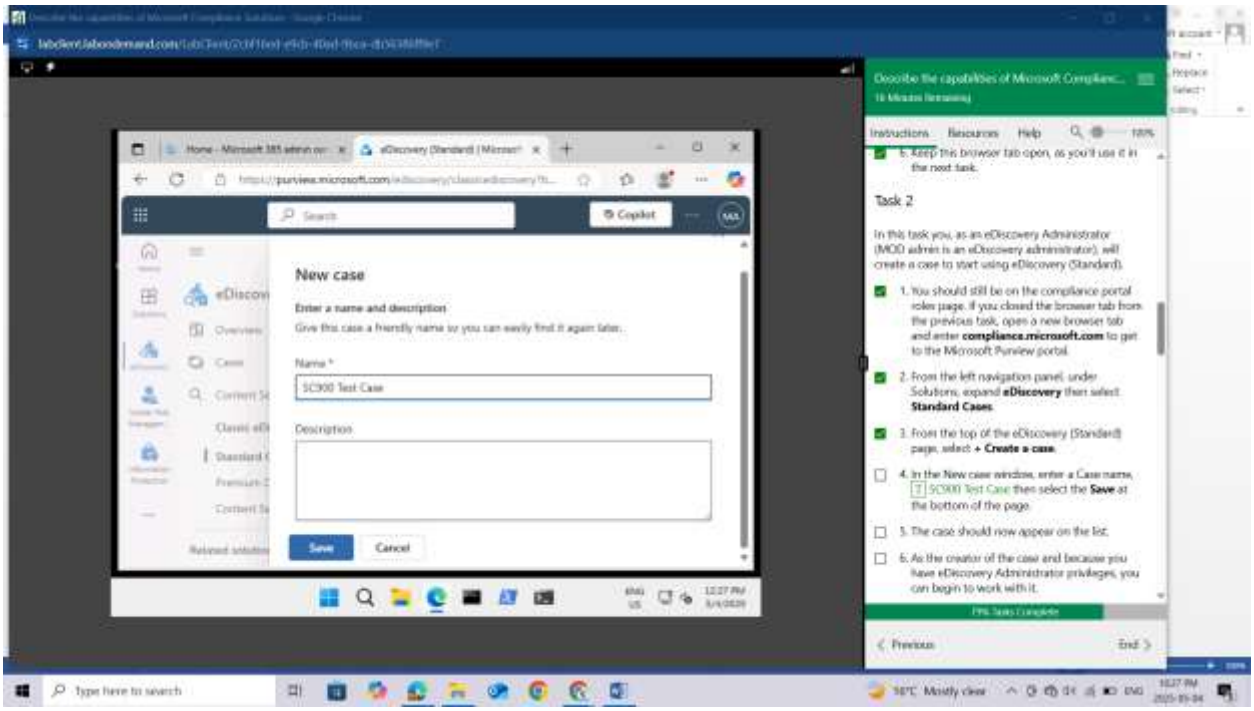
From the left navigation panel, under **Solutions**, expand **eDiscovery** then select **Standard Cases**.



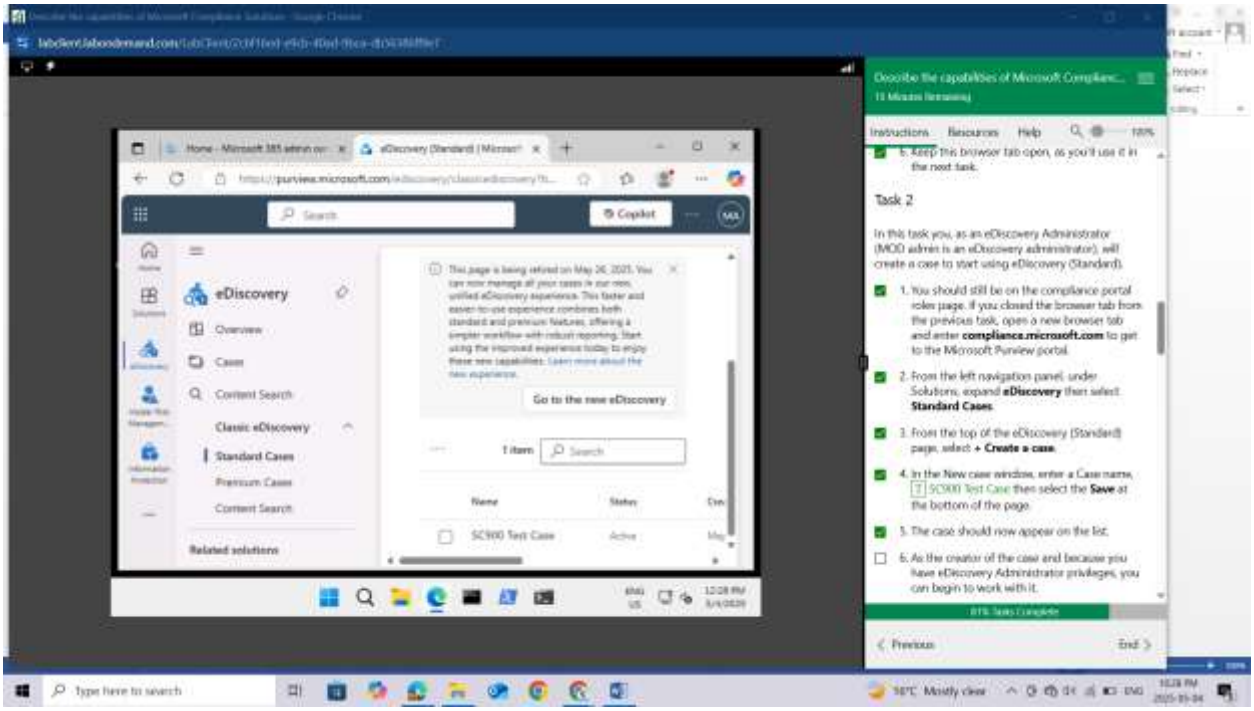

From the top of the eDiscovery (Standard) page, select **+ Create a case.**




In the New case window, enter a **Case name**, ***SC900 Test Case*** then select the **Save** at the bottom of the page.




The case should now appear on the list.




As the creator of the case and because you have eDiscovery Administrator privileges, you can begin to work with it.

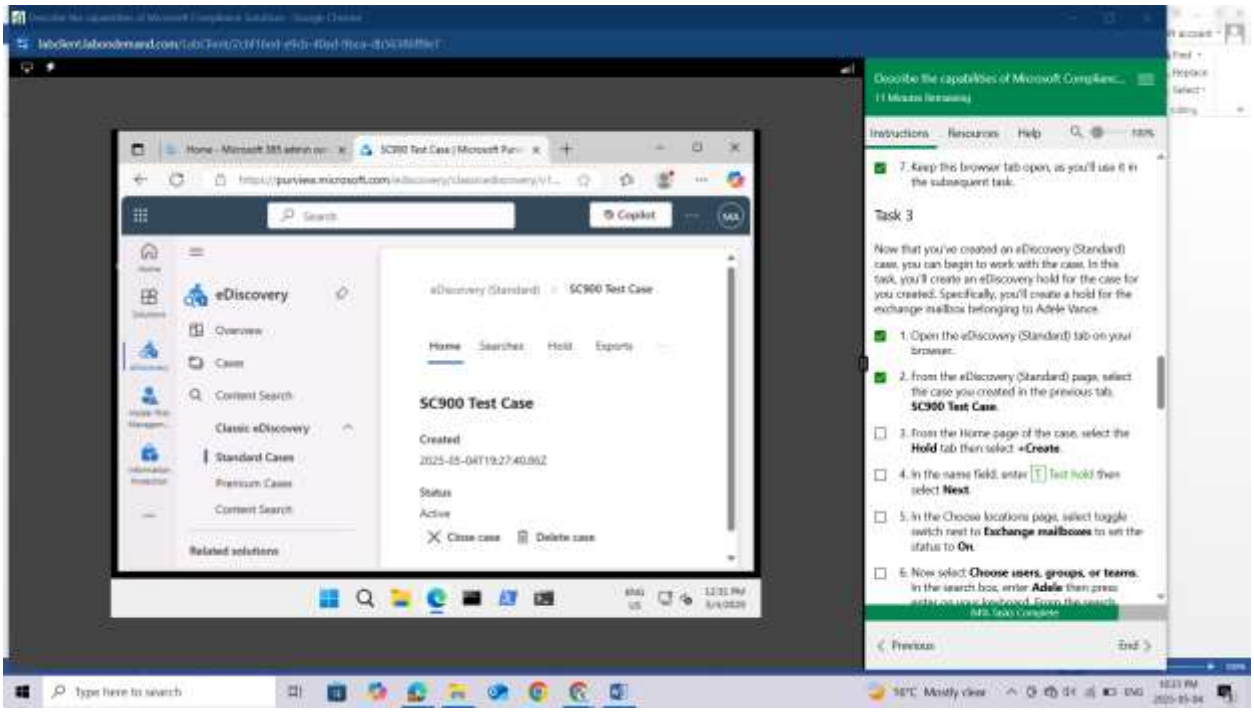
Keep this browser tab open, as you'll use it in the subsequent task.

## Task 3

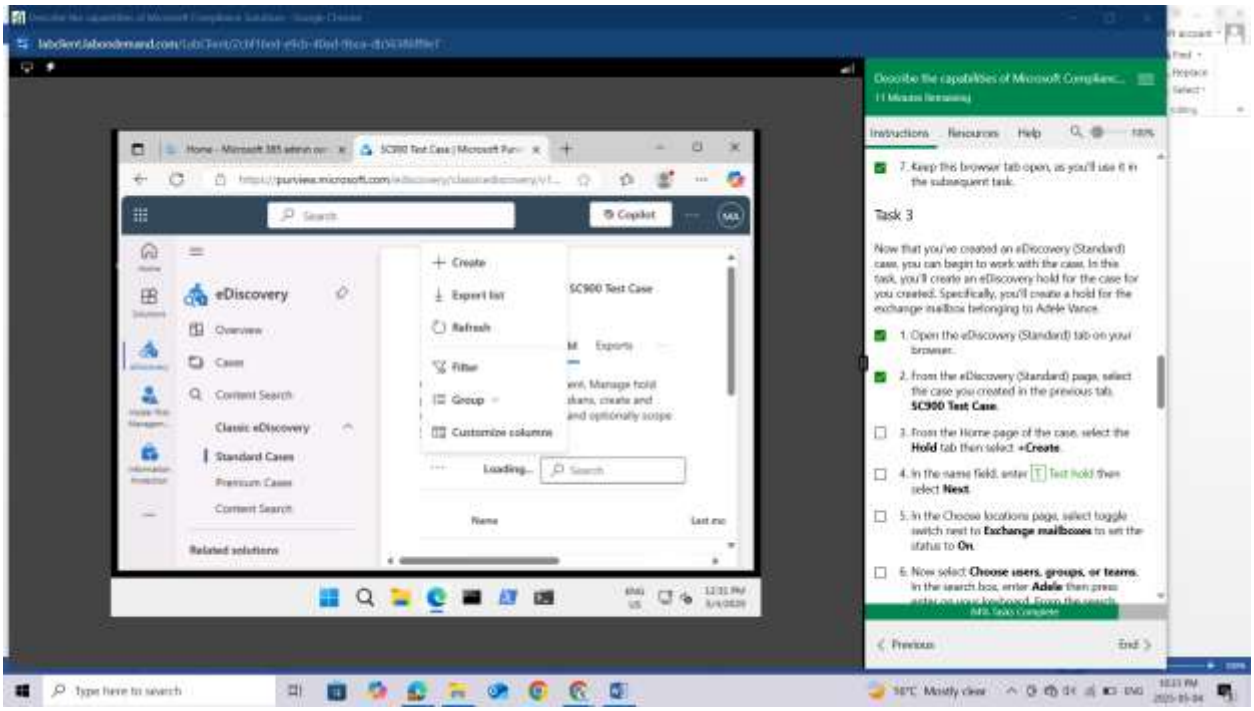
Now that you've created an eDiscovery (Standard) case, you can begin to work with the case. In this task, you'll create an eDiscovery hold for the case for you created. Specifically, you'll create a hold for the exchange mailbox belonging to Adele Vance.

Open the eDiscovery (Standard) tab on your browser.

From the eDiscovery (Standard) page, select the case you created in the previous tab, **SC900 Test Case.**




From the Home page of the case, select the **Hold** tab then select **+Create.**




In the name field, enter **Test hold** then select **Next**.

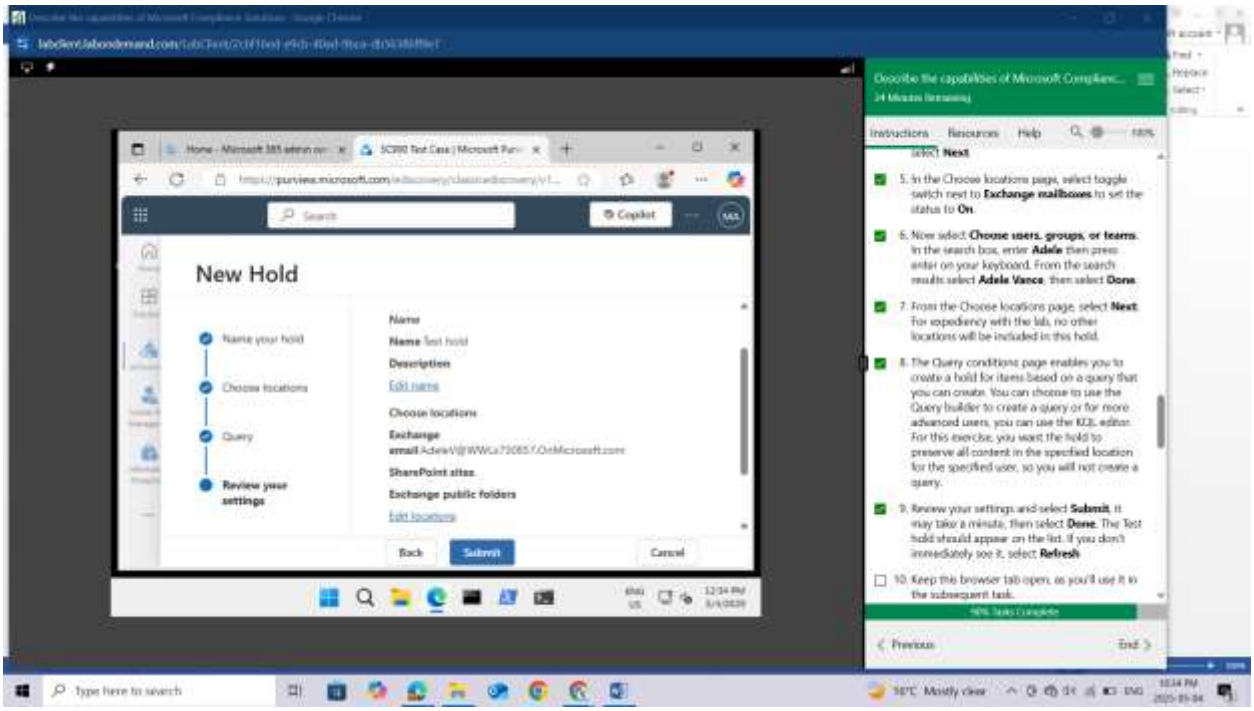
In the Choose locations page, select toggle switch next to Exchange mailboxes to set the status to **On**.

Now select **Choose users, groups, or teams**. In the search box, enter **Adele** then press enter on your keyboard. From the search results select **Adele Vance,** then select **Done**.

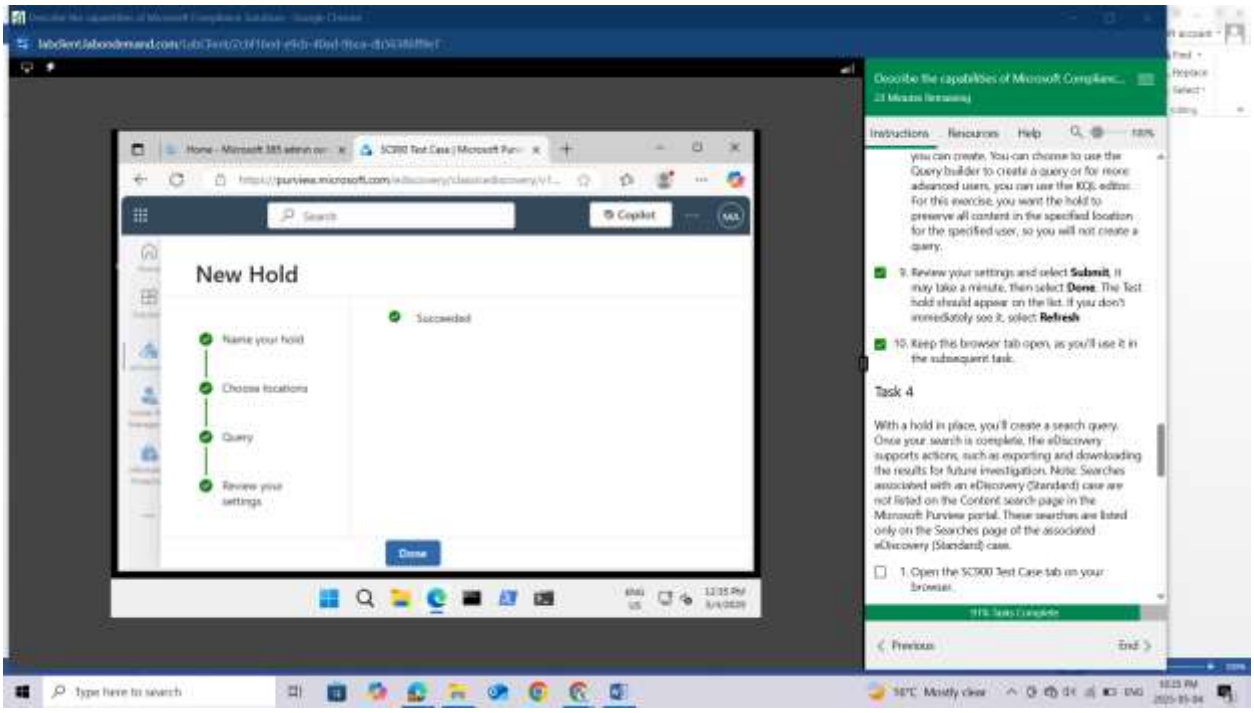
From the Choose locations page, select **Next**. For expediency with the lab, no other locations will be included in this hold.

The Query conditions page enables you to create a hold for items based on a query that you can create. You can choose to use the Query builder to create a query or for more advanced users, you can use the KQL editor. For this exercise, you want the hold to preserve all content in the specified location for the specified user, so you will not create a query.

Review your settings and select **Submit**,




It may take a minute, then select **Done**. The Test hold should appear on the list. If you don't immediately see it, select **Refresh**




Keep this browser tab open, as you'll use it in the subsequent task.

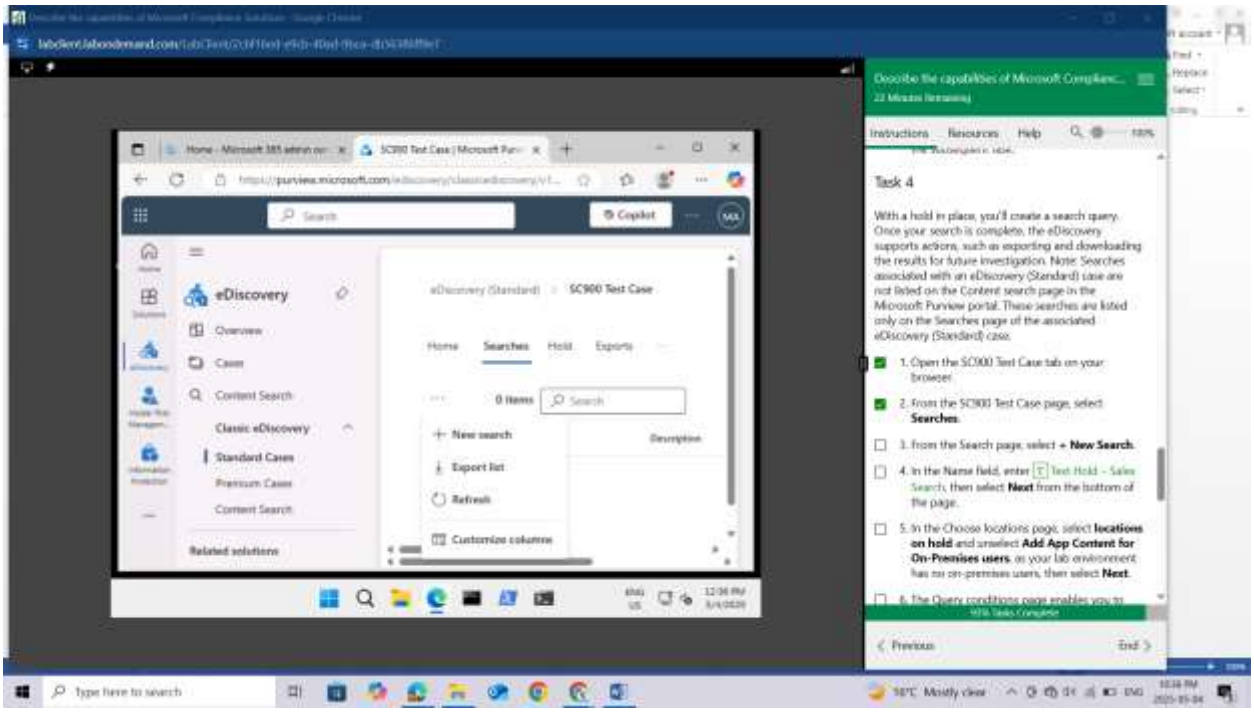
## Task 4

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.

Open the SC900 Test Case tab on your browser.

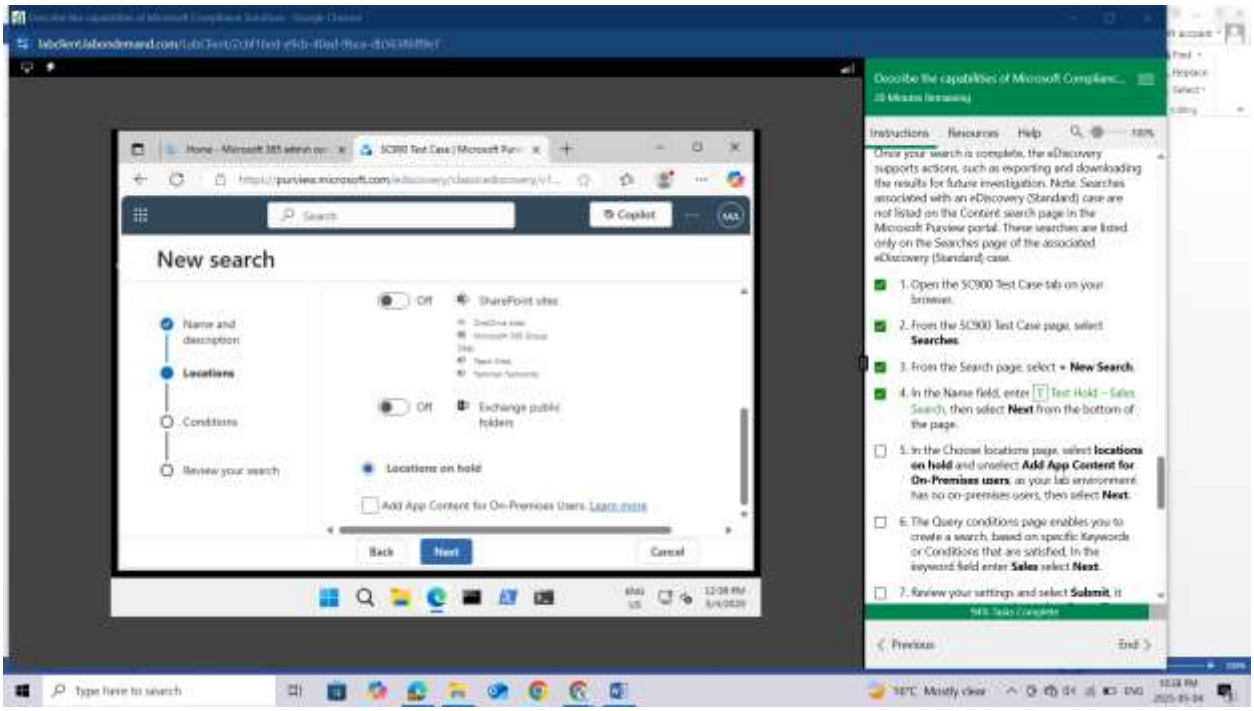
From the SC900 Test Case page, select **Searches**.

From the Search page, select **+ New Search.**

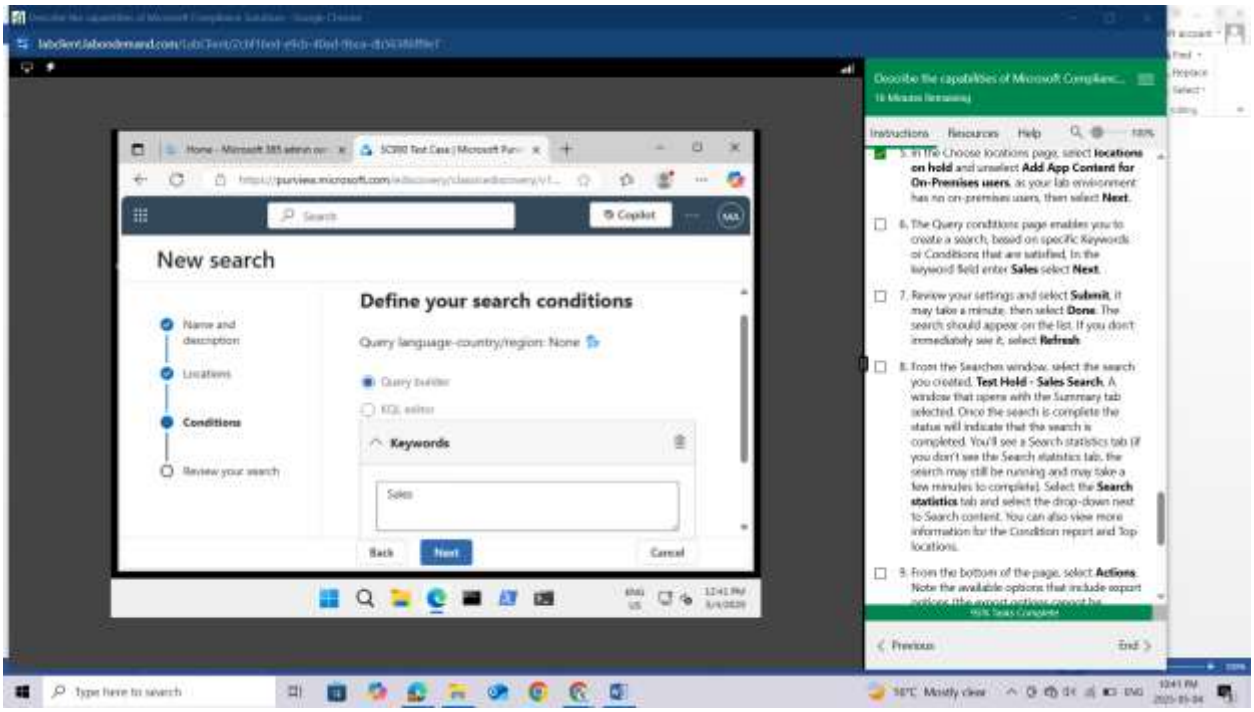



In the Name field, enter **Test Hold – Sales** Search, then select **Next** from the bottom of the page.

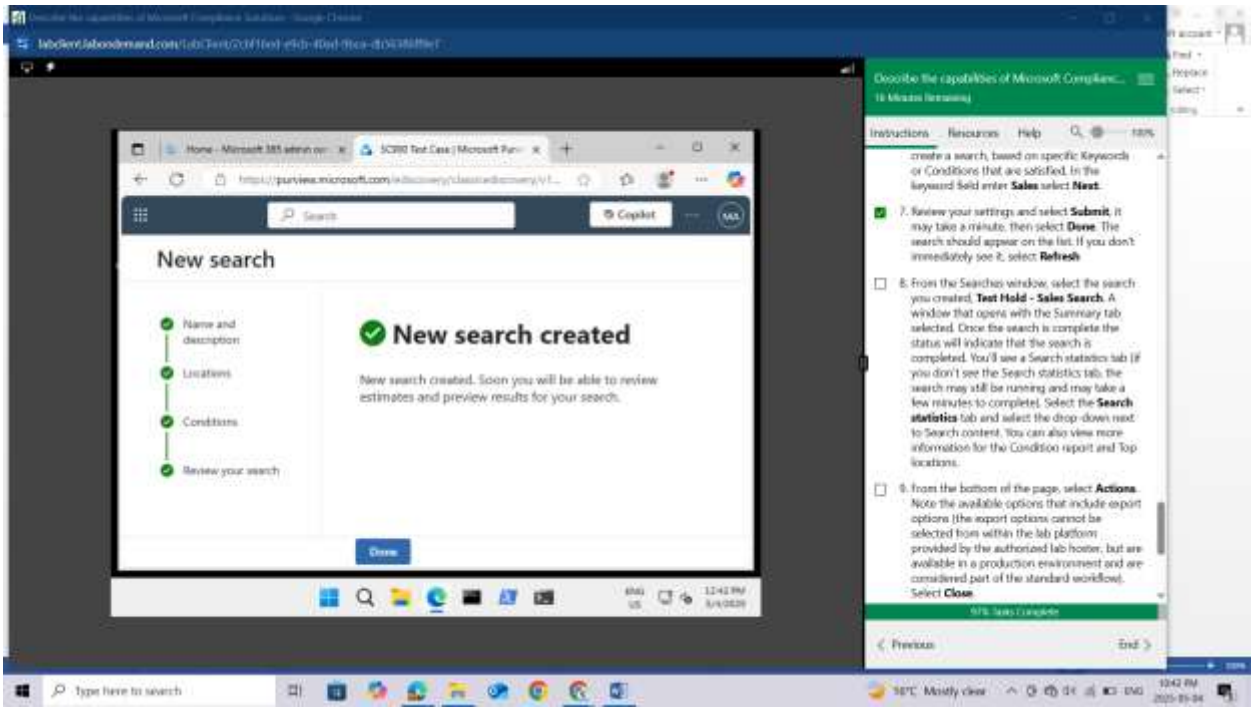
In the Choose locations page, select **locations on hold** and unselect **Add App Content for On-Premises users**, as your lab environment has no on-premises users, then select **Next**



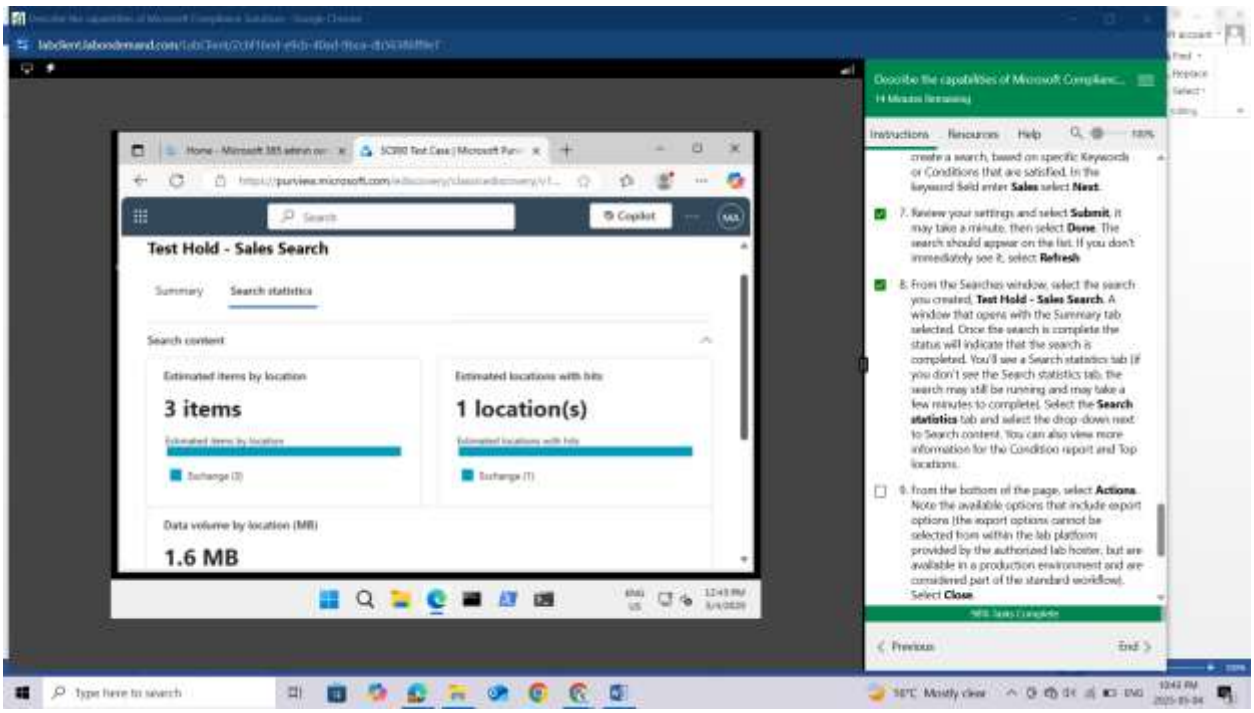

The Query conditions page enables you to create a search, based on specific Keywords or Conditions that are satisfied, In the keyword field enter **Sales** select **Next**.



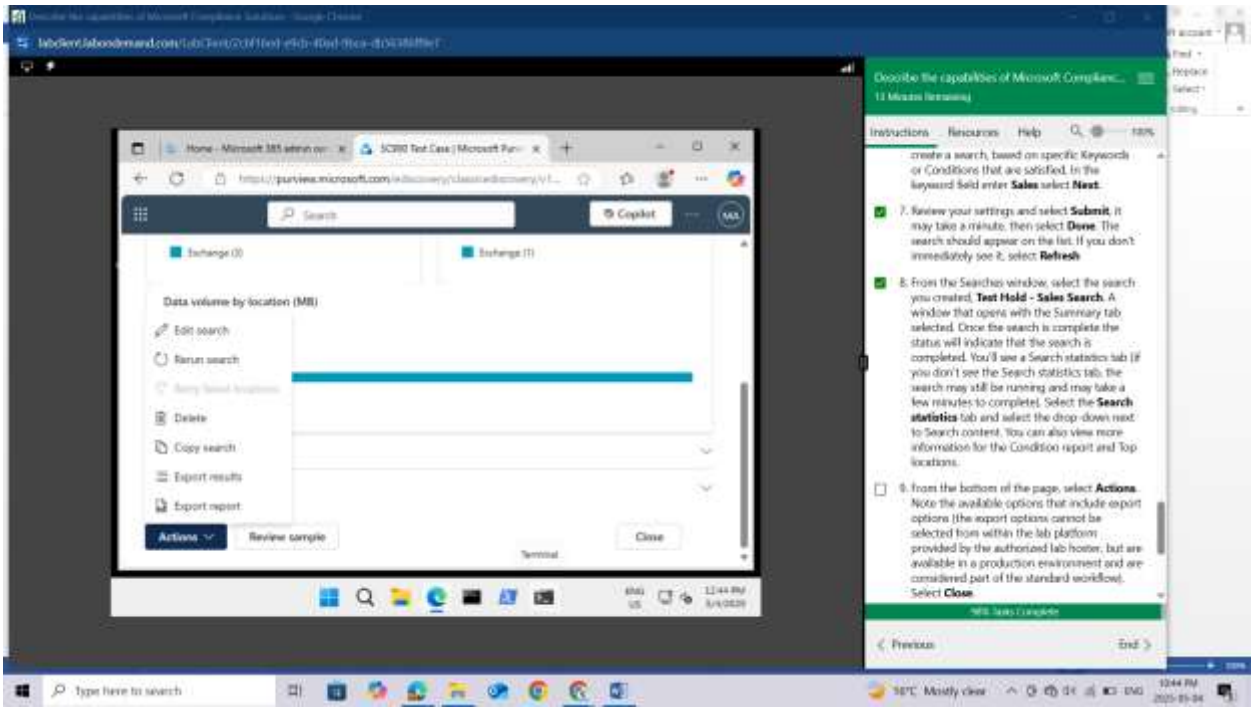

Review your settings and select **Submit**, it may take a minute, then select **Done**. The search should appear on the list. If you don't immediately see it, select **Refresh**

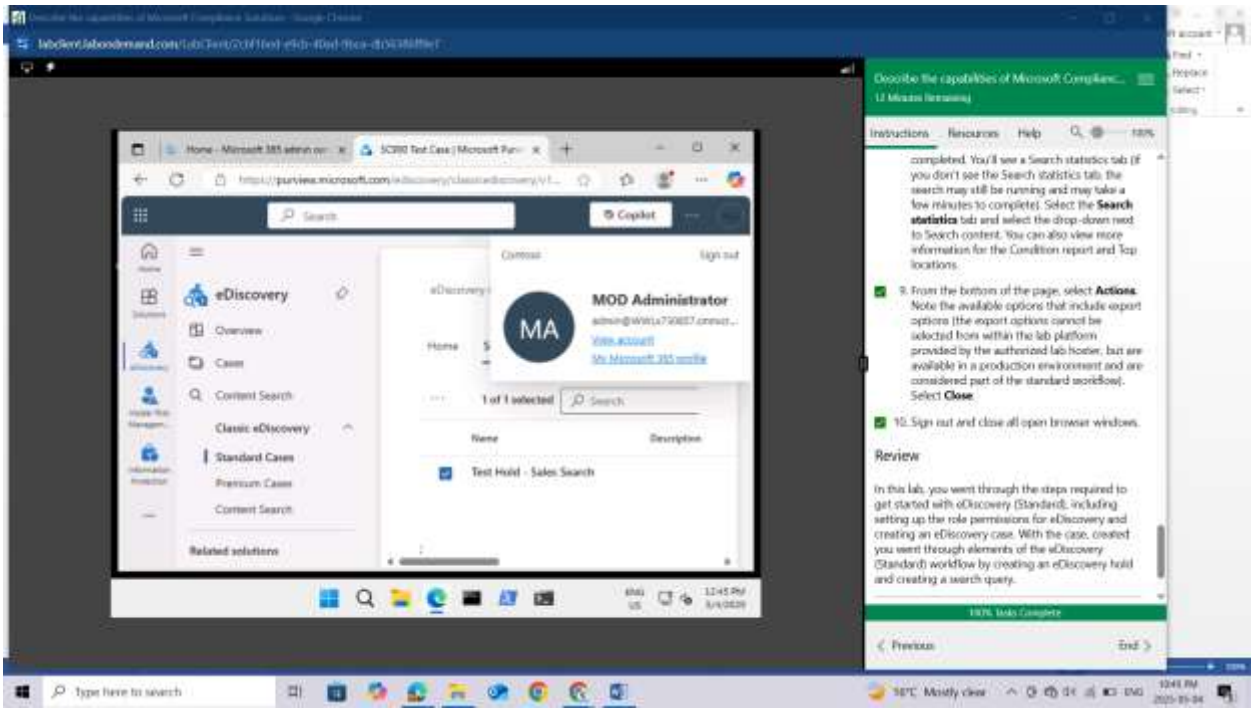



From the Searches window, select the search you created, **Test Hold - Sales Search**. A window that opens with the Summary tab selected. Once the search is complete the status will indicate that the search is completed. You'll see a Search statistics tab (if you don't see the Search statistics tab, the search may still be running and may take a few minutes to complete). Select the Search statistics tab and select the drop-down next to Search content. You can also view more information for the Condition report and Top locations.



From the bottom of the page, select **Actions**. Note the available options that include export options (the export options cannot be selected from within the lab platform provided by the authorized lab hoster, but are available in a production environment and are considered part of the standard workflow). Select **Close**.



## Review

In this lab, you went through the steps required to get started with eDiscovery (Standard), including setting up the role permissions for eDiscovery and creating an eDiscovery case. With the case, created you went through elements of the eDiscovery (Standard) workflow by creating an eDiscovery hold and creating a search query.

# CONCLUSION

By completing these labs, I've established a practical foundation in Microsoft's compliance solutions. I started by setting up a Microsoft 365 tenant, which provided the necessary environment for hands-on exploration. I then examined the Service Trust Portal, gaining insights into Microsoft's commitment to security, compliance, and privacy. The core of my learning centered on the Microsoft Purview portal and Compliance Manager, where I learned to navigate the tools for managing data governance and assessing compliance posture. I further deepened my understanding by working with specific Purview features, including creating and applying sensitivity labels to classify and protect data, exploring insider risk management to identify and mitigate potential threats, and understanding the processes involved in eDiscovery for legal and investigative purposes. Through these labs, I've developed An understanding of how organizations can effectively leverage Microsoft's tools to meet their compliance obligations, safeguard sensitive data, and manage potential risks.