Cyber Shujaa

Cloud Security Specialist

Assignment 5: **Lab: Describe the capabilities of Microsoft Compliance Solutions**

NAME: WELDON KIPKIRUI KENEI

CS NO: ADC-CSS02-25027

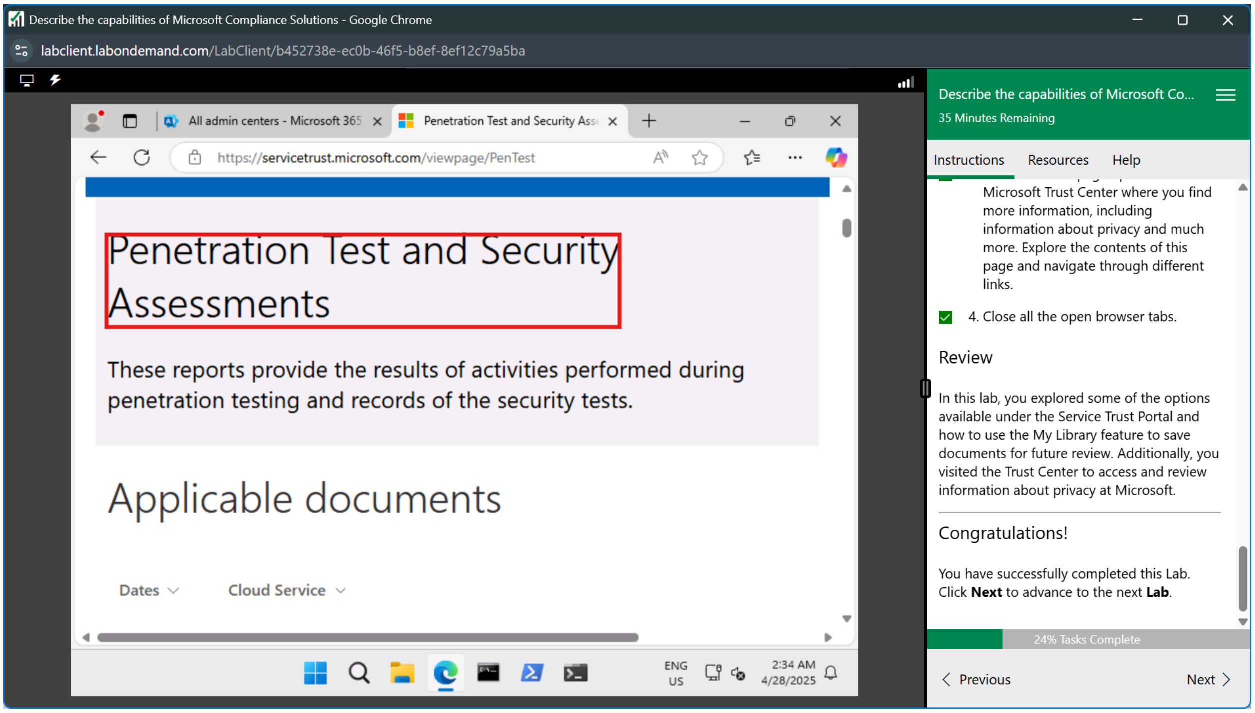
Add Headings (Format > Paragraph styles) and they will appear in your table of contents.

Introduction

In this lab scenario, we will look at the capabilities of Microsoft compliance solutions. Here, we will focus on Microsoft's Service Trust Portal, Purview in risk management, and eDiscovery in managing digital assets and evidence.

Explore the Service Trust Portal

In this portal, we discover how Microsoft Cloud services protect our data and help us manage compliance and data security for our organization.
The following screenshot shows the reports of the penetration tests done on Microsoft cloud services.


Describe the capabilities of Microsoft Compliance Solutions - Google Chrome
labclient.labondemand.com/LabClient/b452738e-ec0b-46f5-b8ef-8ef12c79a5ba
All admin centers - Microsoft 365
Penetration Test and Security Ass
https://servicetrust.microsoft.com/viewpage/PenTest
Dates
Cloud Service
ENG US
2:34 AM 4/28/2025
Describe the capabilities of Microsoft Co...
35 Minutes Remaining
Instructions
Resources
Help
24% Tasks Complete
Previous
Next

Penetration Test and Security Assessments

These reports provide the results of activities performed during penetration testing and records of the security tests.

Applicable documents

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.

☑ 4. Close all the open browser tabs.

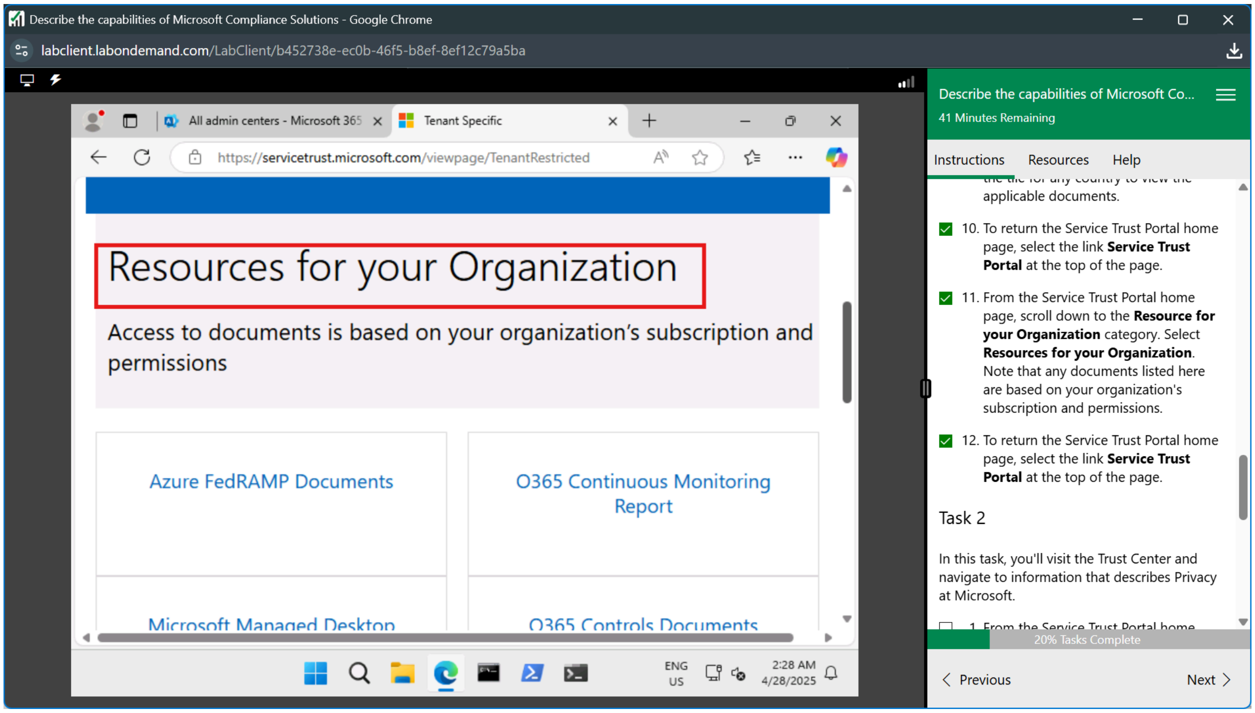
Review

In this lab, you explored some of the options available under the Service Trust Portal and how to use the My Library feature to save documents for future review. Additionally, you visited the Trust Center to access and review information about privacy at Microsoft.

Congratulations!

You have successfully completed this Lab. Click **Next** to advance to the next **Lab**.

We can also manage assets that are based on our organzations subscription and permissions


Describe the capabilities of Microsoft Compliance Solutions - Google Chrome
labclient.labondemand.com/LabClient/b452738e-ec0b-46f5-b8ef-8ef12c79a5ba
All admin centers - Microsoft 365
Tenant Specific
https://servicetrust.microsoft.com/viewpage/TenantRestricted
Azure FedRAMP Documents
O365 Continuous Monitoring Report
Microsoft Managed Desktop
O365 Controls Documents
ENG US
2:28 AM 4/28/2025
Describe the capabilities of Microsoft Co...
41 Minutes Remaining
Instructions
Resources
Help
20% Tasks Complete
Previous
Next

Resources for your Organization

Access to documents is based on your organization's subscription and permissions

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.

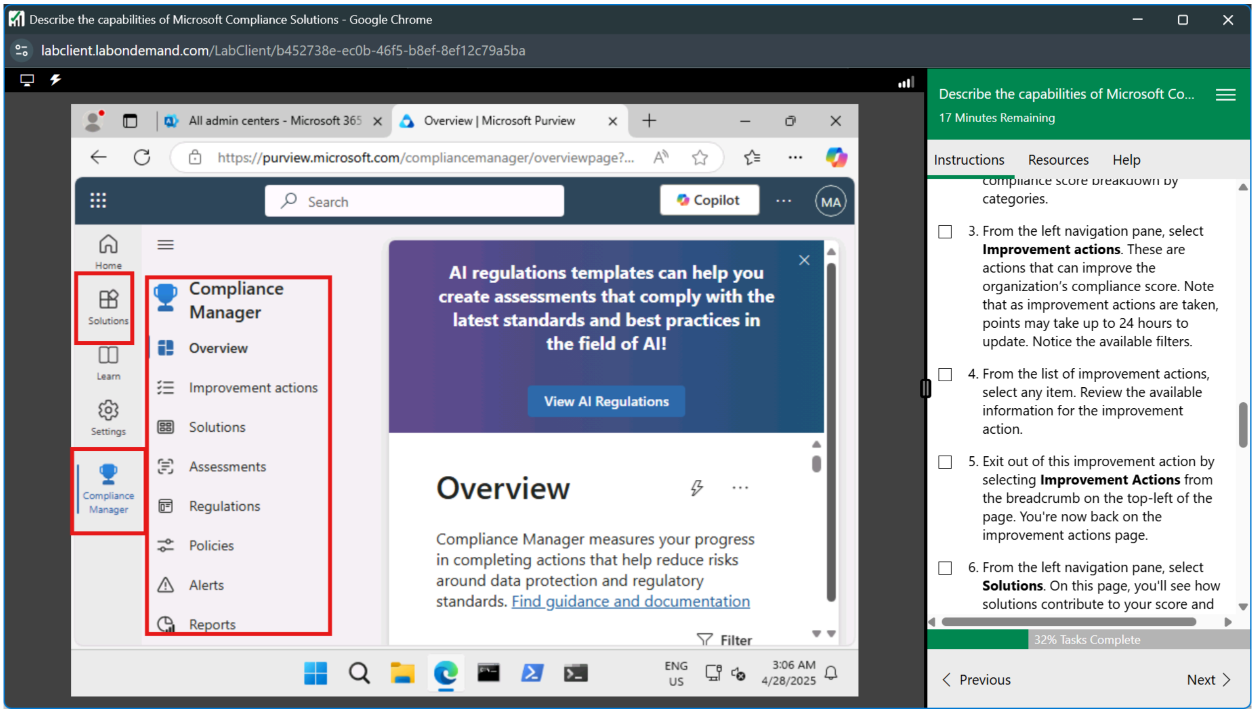
Task 2

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

□ 1. From the Service Trust Portal home

Explore the Microsoft Purview portal and Compliance Manager

In this scenario, we will look at the Microsoft Purview portal and Compliance Manager, on how it can help organizations improve their compliance posture.



Describe the capabilities of Microsoft Compliance Solutions - Google Chrome
labclient.labondemand.com/LabClient/b452738e-ec0b-46f5-b8ef-8ef12c79a5ba
All admin centers - Microsoft 365
Overview | Microsoft Purview
https://purview.microsoft.com/compliancemanager/overviewpage?...
Search
Copilot
MA
Home
Solutions
Learn
Settings
Compliance Manager
Compliance Manager
Overview
Improvement actions
Solutions
Assessments
Regulations
Policies
Alerts
Reports
View AI Regulations
Filter
ENG
US
3:06 AM
4/28/2025
Describe the capabilities of Microsoft Co...
17 Minutes Remaining
Instructions
Resources
Help
32% Tasks Complete
Previous
Next

AI regulations templates can help you create assessments that comply with the latest standards and best practices in the field of AI!

Overview

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

compliance score breakdown by categories.

□ 3. 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.

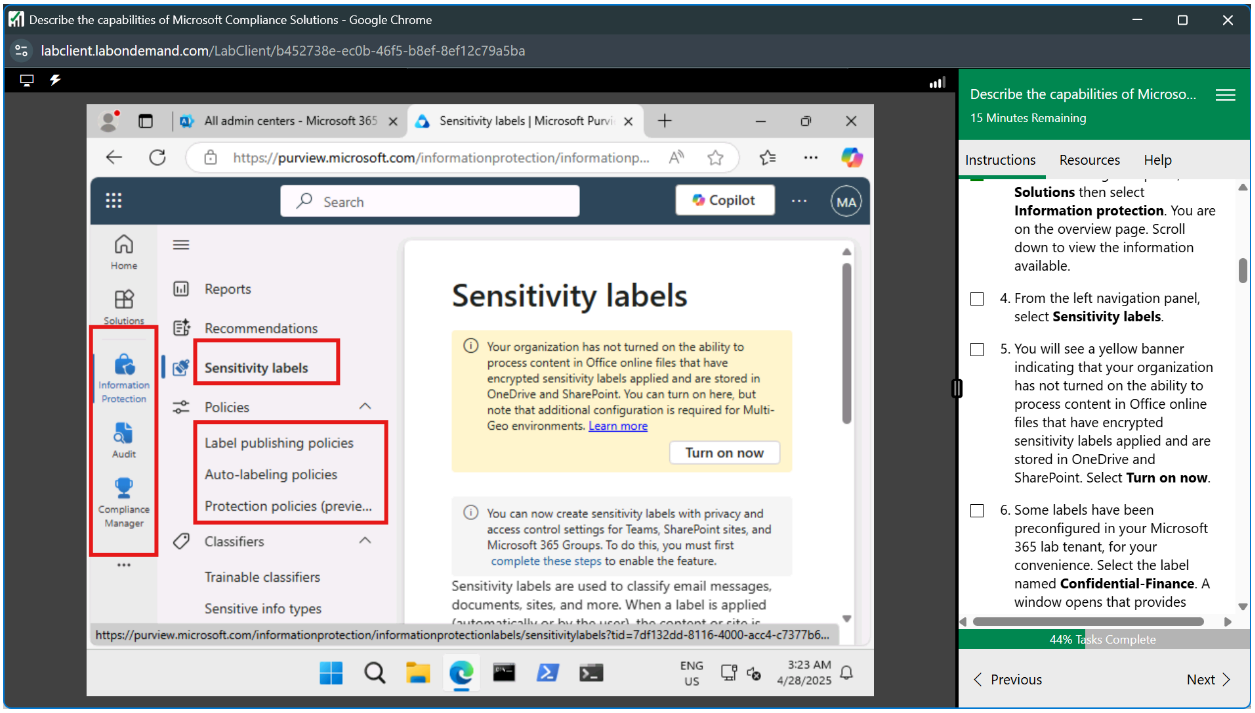
□ 4. From the list of improvement actions, select any item. Review the available information for the improvement action.

□ 5. 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.

□ 6. From the left navigation pane, select **Solutions**. On this page, you'll see how solutions contribute to your score and

Explore sensitivity labels in Microsoft Purview

Here, we will explore the capabilities of sensitivity labels. We'll go through the settings for existing sensitivity labels that have been created and the corresponding policy to publish the label. Then we'll see how to apply a label and the impact of that label, from the perspective of a user.


Describe the capabilities of Microsoft Compliance Solutions - Google Chrome
labclient.labondemand.com/LabClient/b452738e-ec0b-46f5-b8ef-8ef12c79a5ba
All admin centers - Microsoft 365
Sensitivity labels | Microsoft Purview
https://purview.microsoft.com/informationprotection/informationp...
Search
Copilot
MA
Home
Solutions
Information Protection
Audit
Compliance Manager
Reports
Recommendations
Sensitivity labels
Policies
Label publishing policies
Auto-labeling policies
Protection policies (previe...
Classifiers
Trainable classifiers
Sensitive info types
https://purview.microsoft.com/informationprotection/informationprotectionlabels/sensitivitylabels?tid=7df132dd-8116-4000-acc4-c7377b6...
ENG US
3:23 AM 4/28/2025
Instructions
Resources
Help
44% Tasks Complete
Previous
Next

Sensitivity labels

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. You can turn on here, but note that additional configuration is required for Multi-Geo environments. Learn more

Turn on now

You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first complete these steps to enable the feature.

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is

Describe the capabilities of Microso...

15 Minutes Remaining

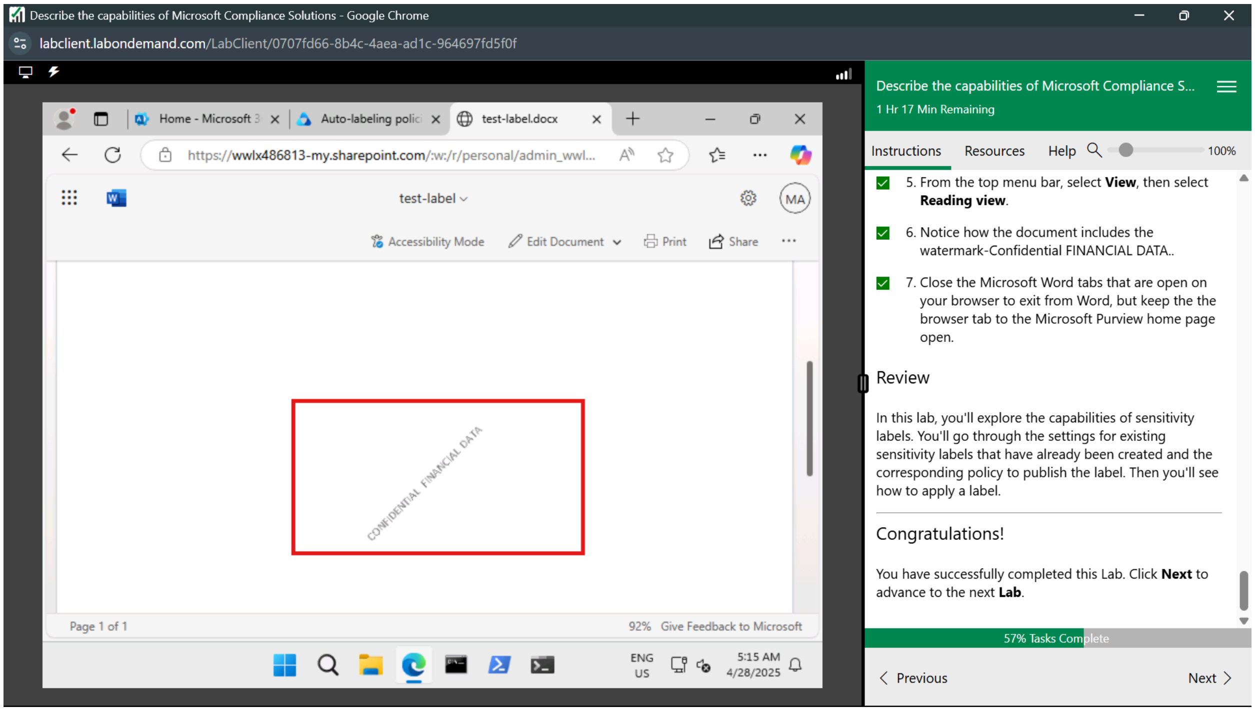
Solutions then select **Information protection**. You are on the overview page. Scroll down to view the information available.

□ 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

We then created a word document with sensitivity label as follows


Describe the capabilities of Microsoft Compliance Solutions - Google Chrome
labclient.labondemand.com/LabClient/0707fd66-8b4c-4aea-ad1c-964697fd5f0f
Home - Microsoft 3
Auto-labeling polic
test-label.docx
https://wwlx486813-my.sharepoint.com/:w:/r/personal/admin_wwl...
test-label
MA
Accessibility Mode
Edit Document
Print
Share
CONFIDENTIAL FINANCIAL DATA
Page 1 of 1
92%
Give Feedback to Microsoft
ENG US
5:15 AM 4/28/2025
Instructions
Resources
Help
100%
57% Tasks Complete
Previous
Next

Describe the capabilities of Microsoft Compliance S...

1 Hr 17 Min Remaining

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

☑ 6. Notice how the document includes the watermark-Confidential FINANCIAL DATA..

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

Review

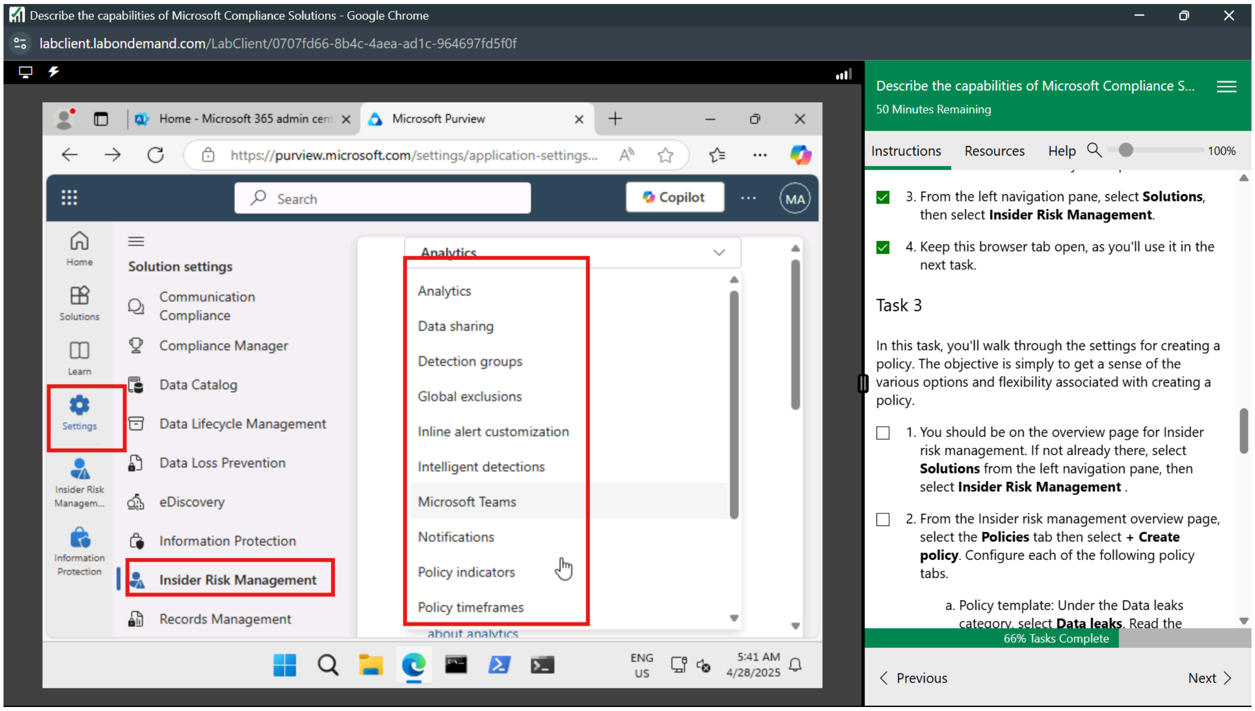
In this lab, you'll explore the capabilities of sensitivity labels. You'll go through the settings for existing sensitivity labels that have already been created and the corresponding policy to publish the label. Then you'll see how to apply a label.

Congratulations!

You have successfully completed this Lab. Click **Next** to advance to the next **Lab**.

Explore insider risk management in Microsoft Purview

In this task, we will walk through the process of setting up an insider risk policy, along with the basic prerequisites to configure and use insider risk management policies.



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

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

Task 3

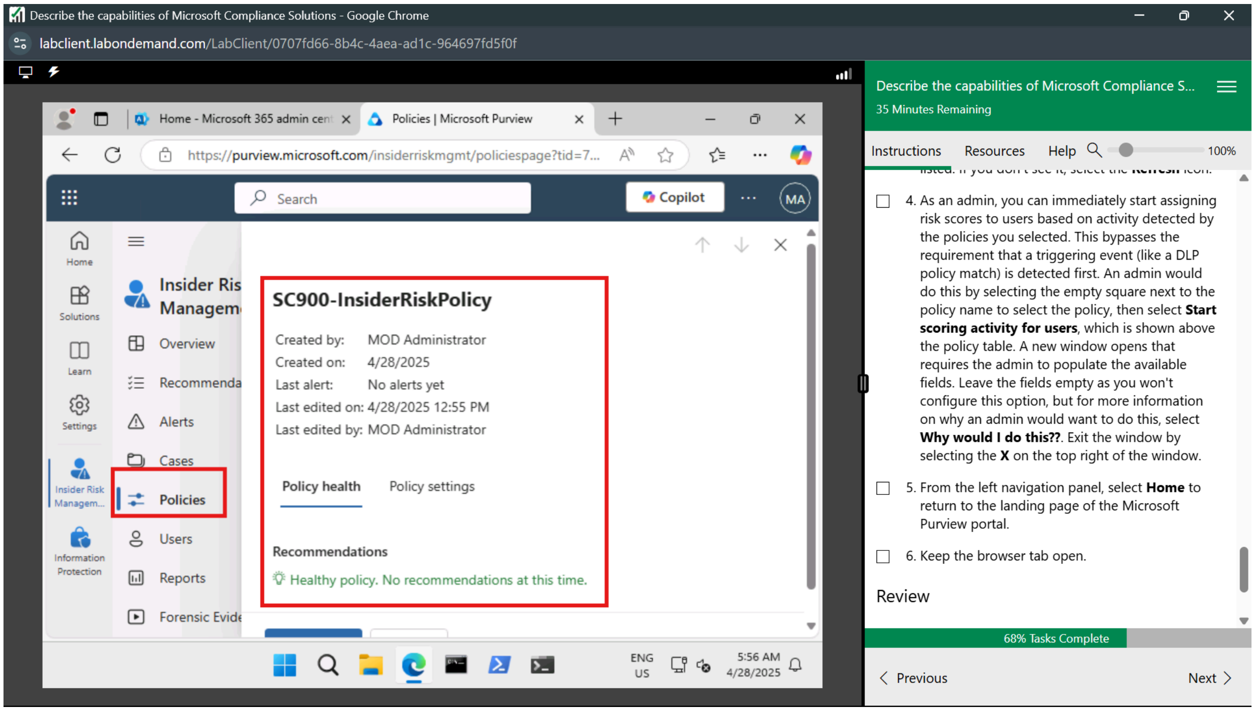
In this task, you'll walk through the settings for creating a policy. The objective is simply to get a sense of the various options and flexibility associated with creating a policy.

□ 1. 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** .

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

a. Policy template: Under the Data leaks category, select **Data leaks**. Read the

We then created a custom insider risk policy based on DLP.


Describe the capabilities of Microsoft Compliance Solutions - Google Chrome
labclient.labondemand.com/LabClient/0707fd66-8b4c-4aea-ad1c-964697fd5f0f
Home - Microsoft 365 admin cent
Policies | Microsoft Purview
https://purview.microsoft.com/insiderriskmgmt/policiespage?tid=7...
Search
Copilot
MA
Home
Solutions
Learn
Settings
Insider Risk Managem...
Information Protection
Insider Risk Management
Overview
Recommenda
Alerts
Cases
Policies
Users
Reports
Forensic Evide
ENG US
5:56 AM 4/28/2025
Describe the capabilities of Microsoft Compliance S...
35 Minutes Remaining
Instructions
Resources
Help
100%
68% Tasks Complete
Previous
Next

SC900-InsiderRiskPolicy

Created by: MOD Administrator
Created on: 4/28/2025
Last alert: No alerts yet
Last edited on: 4/28/2025 12:55 PM
Last edited by: MOD Administrator

Policy health | Policy settings

Recommendations

Healthy policy. No recommendations at this time.

listed. If you don't see it, select the **Refresh** icon.

□ 4. 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.

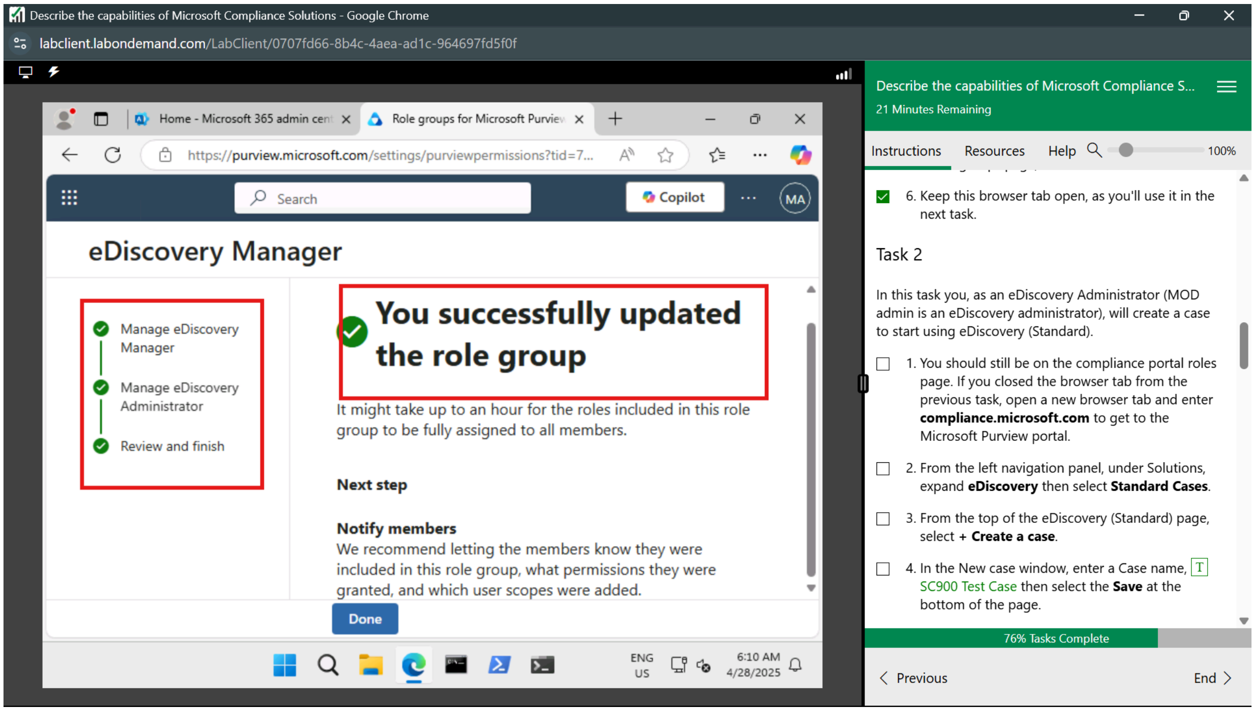
□ 5. From the left navigation panel, select **Home** to return to the landing page of the Microsoft Purview portal.

□ 6. Keep the browser tab open.

Review

Explore eDiscovery

In this task, we will 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.We created a role group to allow a user to create and access an eDiscovery case.


Describe the capabilities of Microsoft Compliance Solutions - Google Chrome
labclient.labondemand.com/LabClient/0707fd66-8b4c-4aea-ad1c-964697fd5f0f
Home - Microsoft 365 admin cent
Role groups for Microsoft Purview
https://purview.microsoft.com/settings/purviewpermissions?tid=7...
Search
Copilot
MA
Done
ENG US
6:10 AM 4/28/2025
Describe the capabilities of Microsoft Compliance S...
21 Minutes Remaining
Instructions
Resources
Help
100%
76% Tasks Complete
Previous
End

eDiscovery Manager

- ✓ Manage eDiscovery Manager
- ✓ Manage eDiscovery Administrator
- ✓ Review and finish

You successfully updated the role group

It might take up to an hour for the roles included in this role group to be fully assigned to all members.

Next step

Notify members

We recommend letting the members know they were included in this role group, what permissions they were granted, and which user scopes were added.

☑ 6. 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).

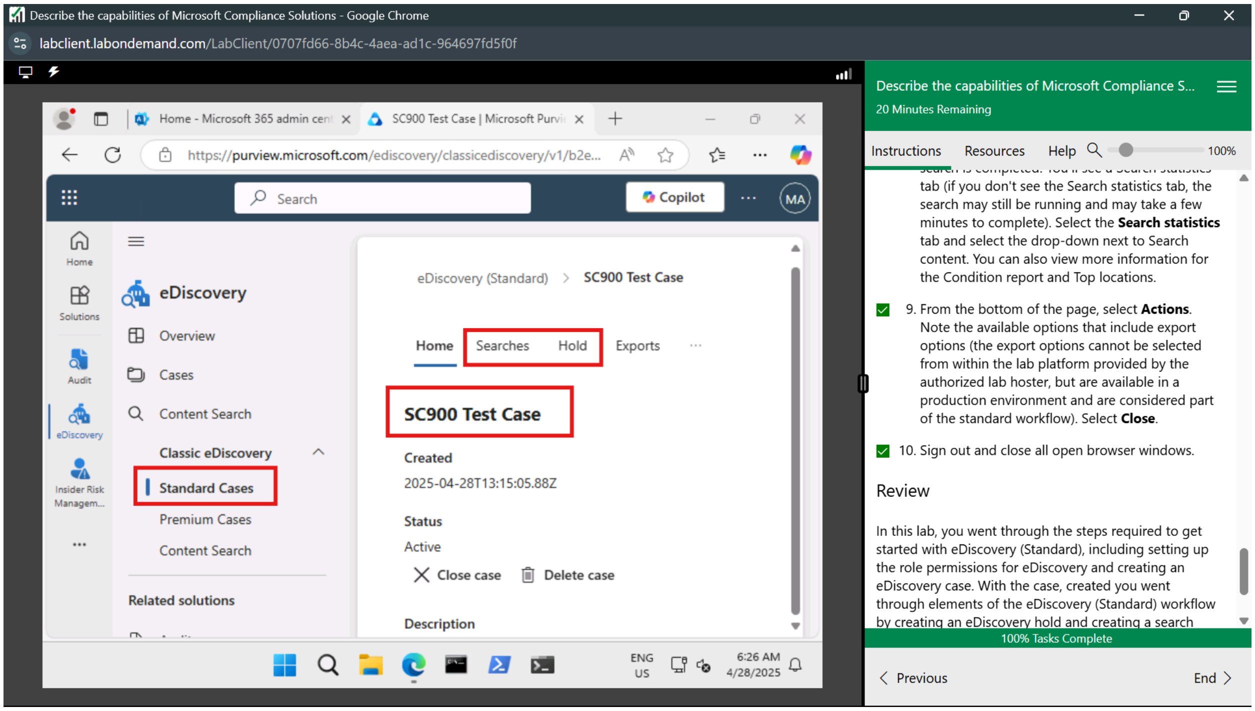
☐ 1. You should still be on the compliance portal roles page. If you closed the browser tab from the previous task, open a new browser tab and enter **compliance.microsoft.com** to get to the Microsoft Purview portal.

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

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

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

From our test case, we were able to create holds and searches to get the exact information we required for a case.


Describe the capabilities of Microsoft Compliance Solutions - Google Chrome
labclient.labondemand.com/LabClient/0707fd66-8b4c-4aea-ad1c-964697fd5f0f
Home - Microsoft 365 admin cent
SC900 Test Case | Microsoft Purvi
https://purview.microsoft.com/ediscovery/classicediscovery/v1/b2e...
Search
Copilot
MA
Home
Solutions
Audit
eDiscovery
Insider Risk Managem...
eDiscovery
Overview
Cases
Content Search
Classic eDiscovery
Standard Cases
Premium Cases
Content Search
Related solutions
eDiscovery (Standard) > SC900 Test Case
Home
Searches
Hold
Exports
Close case
Delete case
ENG US
6:26 AM 4/28/2025
Describe the capabilities of Microsoft Compliance S...
20 Minutes Remaining
Instructions
Resources
Help
100%
100% Tasks Complete
Previous
End

SC900 Test Case

Created

2025-04-28T13:15:05.88Z

Status

Active

Description

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.

☑ 9. 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**.

☑ 10. Sign out and close all open browser windows.

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

Conclusion

In conclusion, we have seen Microsoft’s Purview data security capabilities, such as sensitivity labeling that ensures data monitoring across an organization’s digital estate. We have also explored its capability of risk management, especially insider risk, by monitoring the actions of users and data. Finally, we managed to explore the eDiscovery capability to export data for evidence and audit using case files, hold, and search technologies.