NAME: STEPHEN KYALO -ADC-DP01-25005

PROGRAM: DATA PROTECTION SPECIALIST

CLOUD SLICE TOPIC: MANAGE COMPLIANCE ROLES & MANAGE SENSITIVE INFORMATION TYPES COMPLETION REQUIREMENTS

EXECUTIVE SUMMARY

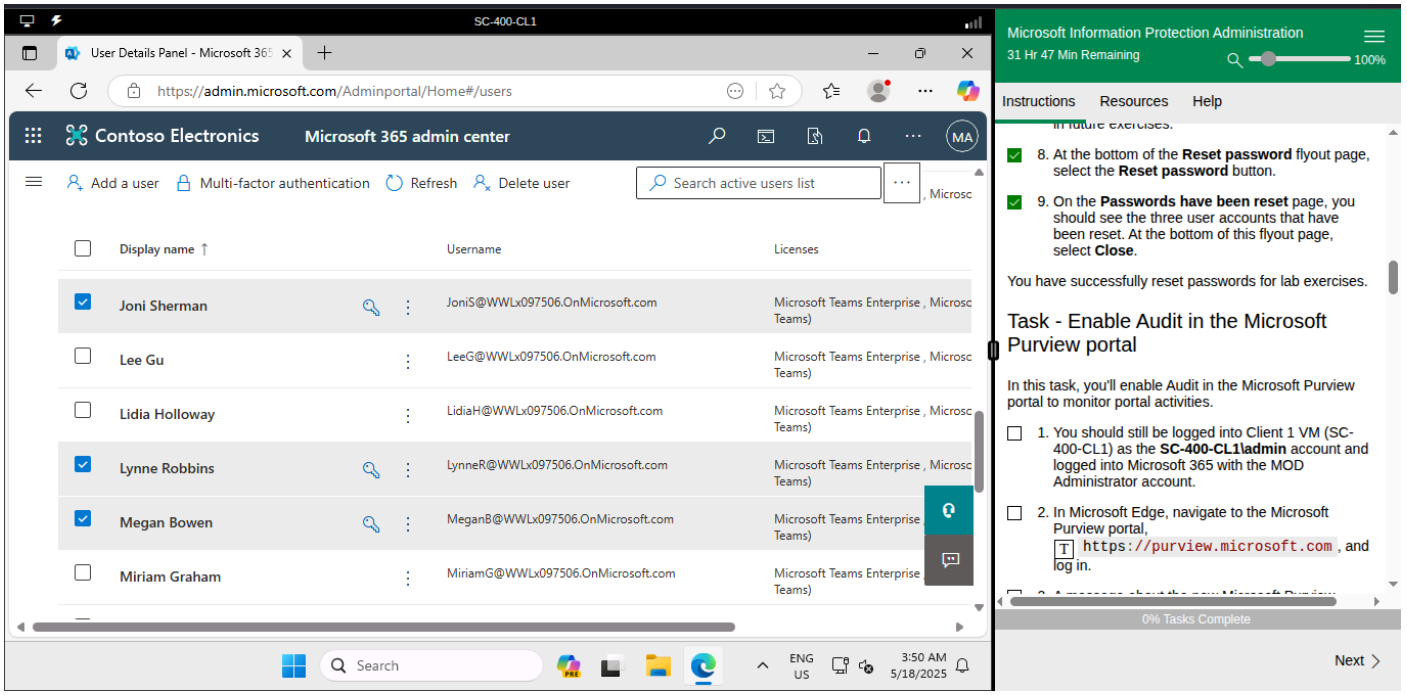
The lab setup and environment preparation in Microsoft Purview involve configuring essential compliance and security settings. The process begins with resetting the passwords for three key users: Joni Sherman, Lynne Robbins, and Morgan Bowen. This step is crucial for establishing secure user access.

Next, auditing is enabled through the Purview portal or PowerShell to monitor user activity. The "Search by Name" feature is activated in Microsoft Teams to facilitate user identification, which is essential for configuring information barriers. These barriers are also enabled in SharePoint Online and OneDrive using PowerShell to ensure secure file collaboration.

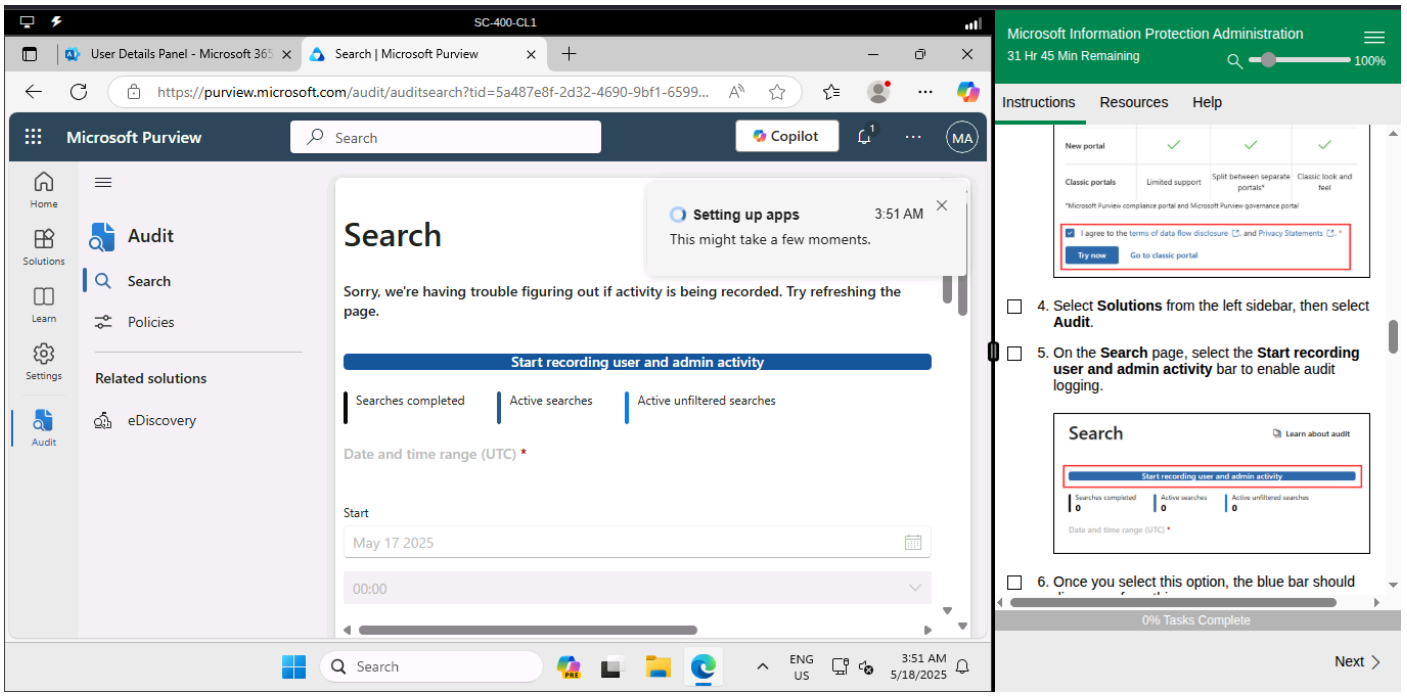
Joni Sherman is assigned the Compliance Administrator role, which grants her the ability to manage compliance features across Microsoft 365. Additionally, the lab covers the management of Sensitive Information Types (SITs), including built-in, named entity, custom, and exact data match types, to aid in detecting and classifying sensitive data within the organisation.

1. LAB SETUP AND ENVIRONMENT PREPARATION

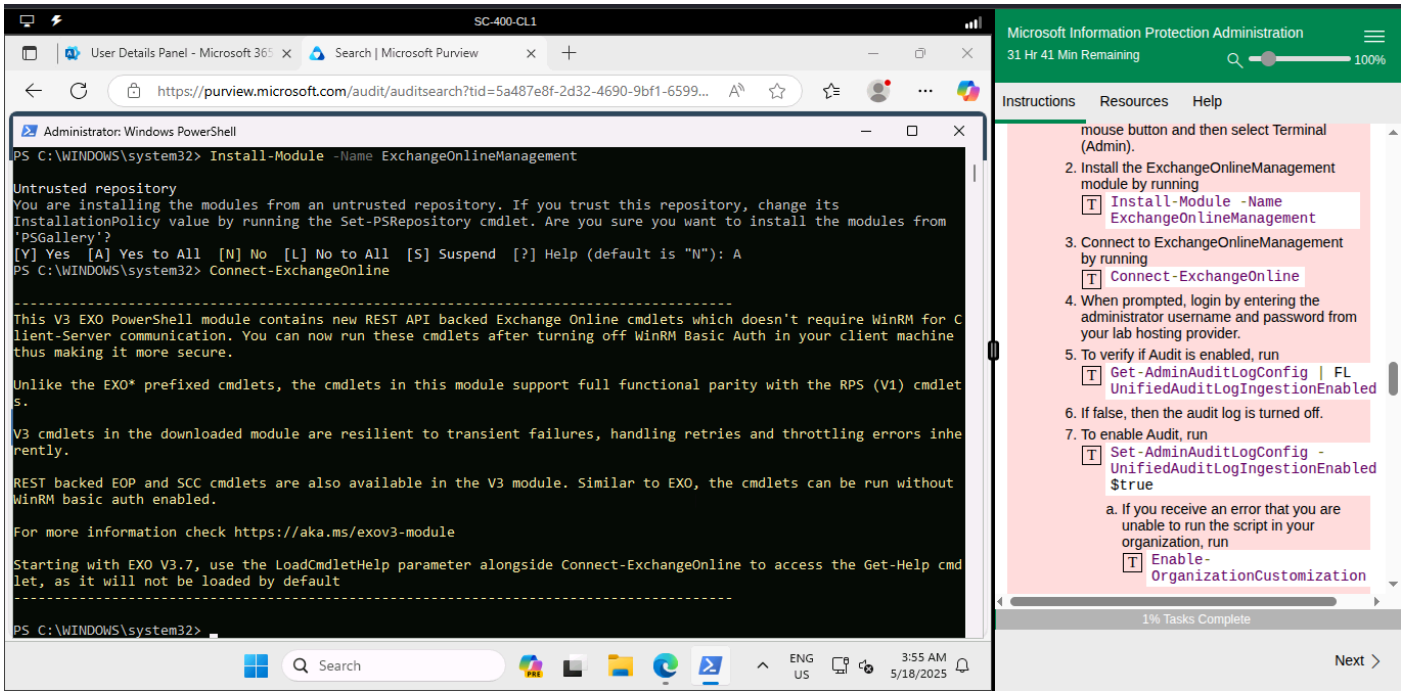
This stage evolves around configuring and preparing the cloud environment for administrative tasks. The process begins with resetting the passwords of three users: Joni Sherman, Lynne Robbins, and Morgan Bowen. Each user account is assigned a single custom password as shown below.



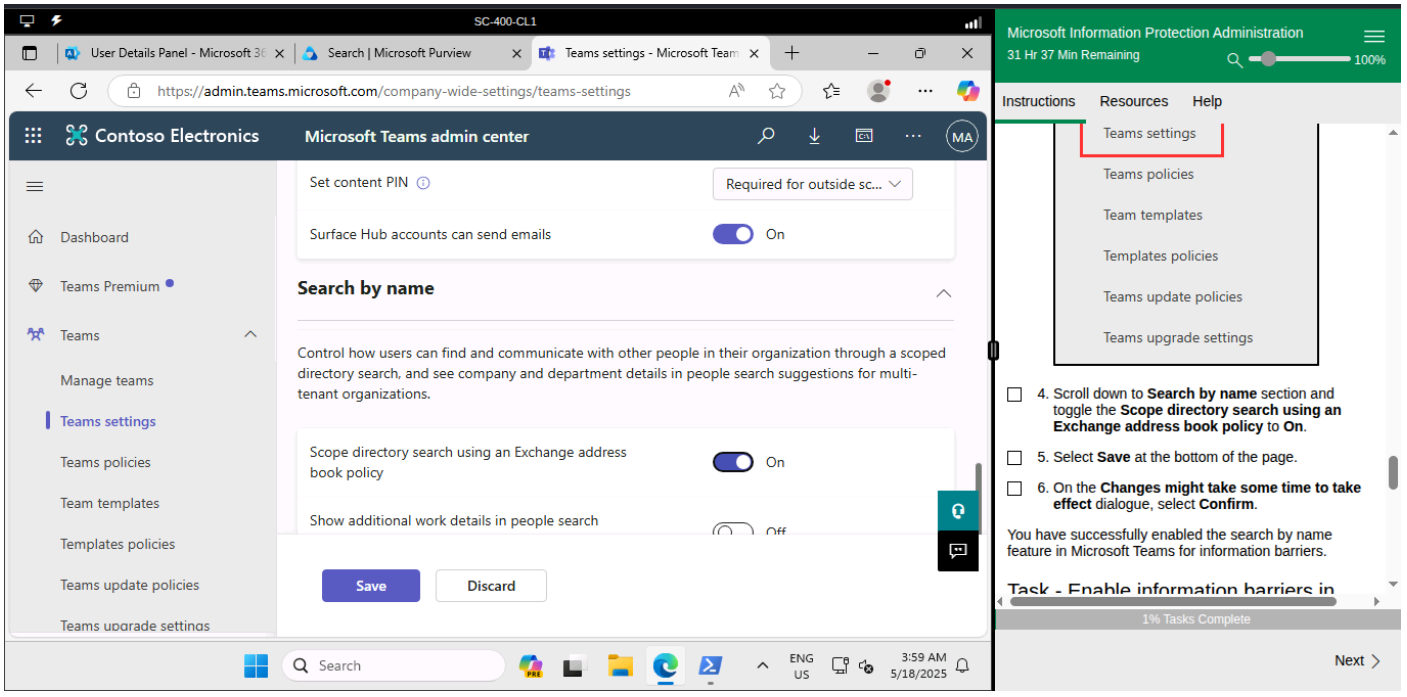
The next step is to enable Auditing through the Audit feature in the Purview Portal. This allows monitoring of the Purview portal activities.



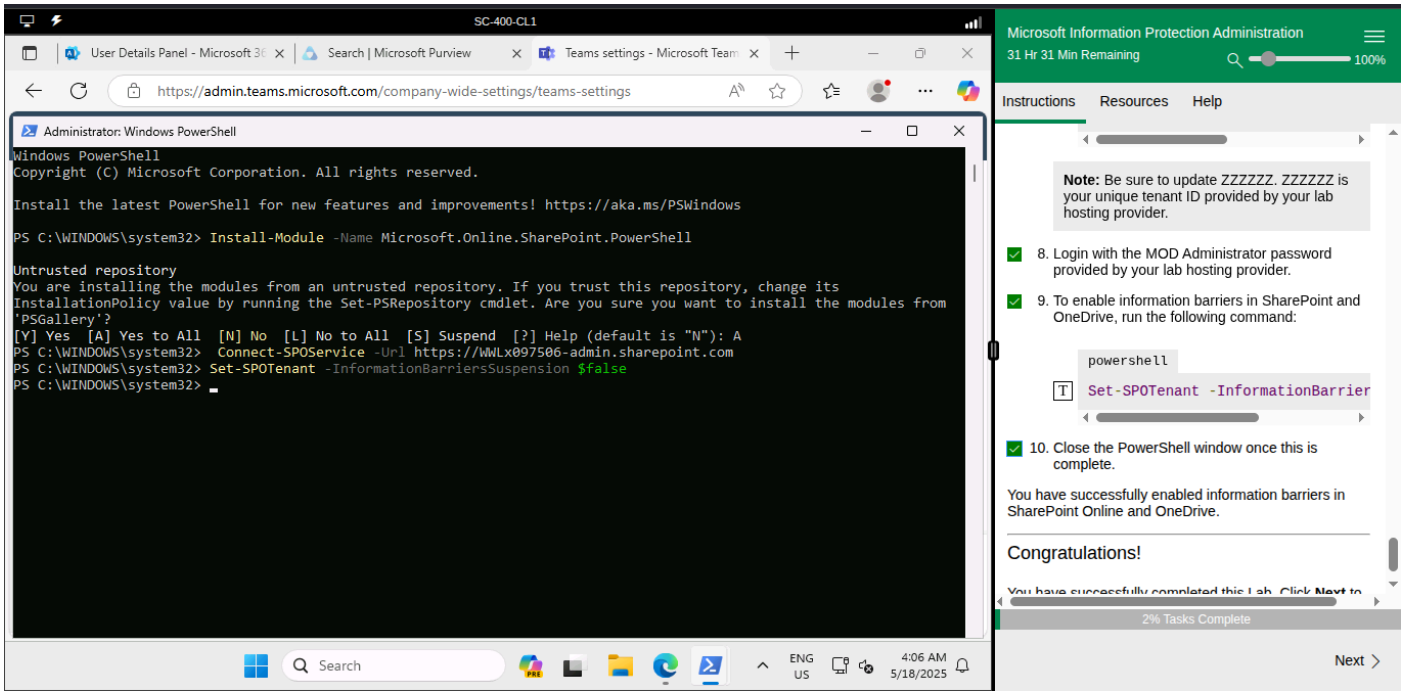
Auditing can also be enabled through PowerShell with elevated privileges if enabling it through the portal fails.



Next is enabling the **Search by name** feature in Microsoft Teams to enable easy user location. Search by name is enabled through the Microsoft Teams Admin center. This is needed for configuring information barriers later on in the lab exercise.

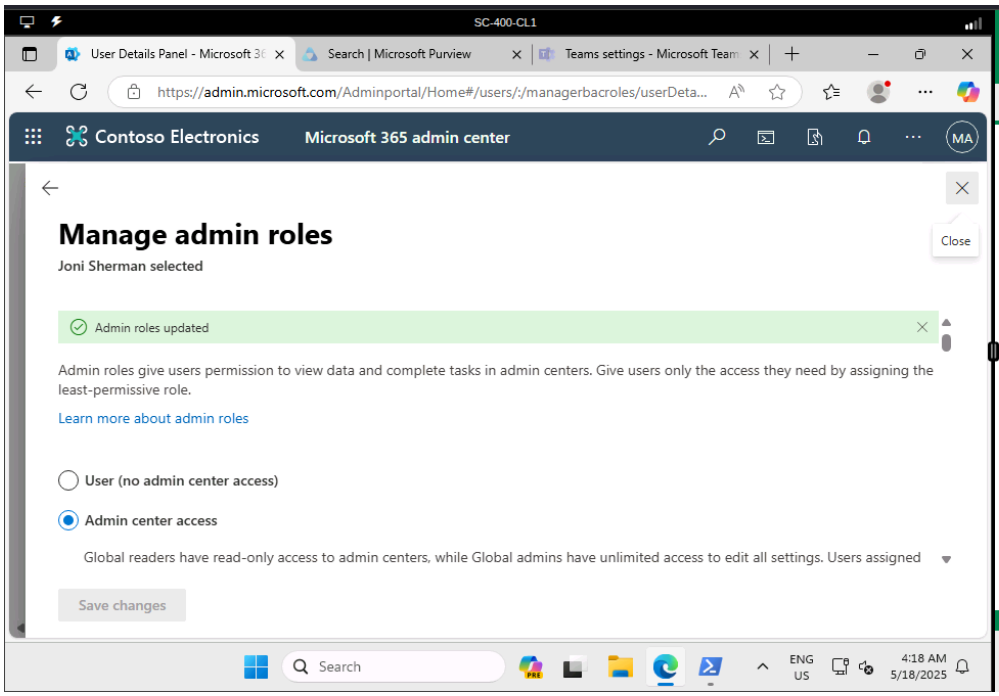


After enabling the **Search by name** feature, we need to enable Information barriers in SharePoint Online and OneDrive through PowerShell. This ensures the security of collaboration files stored in both OneDrive and SharePoint.



2. MANAGE COMPLIANCE ROLES

The user Joni Sherman is assigned Compliance Administrator roles and given access to admin centres. The Compliance Administrator role enables Joni to **manage compliance-related features and data** across Microsoft 365. This role is especially useful for those responsible for overseeing regulatory compliance, risk management, and data protection. This is demonstrated below.



Microsoft Information Protection Administration

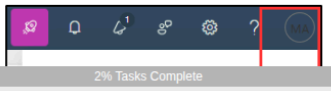
31 Hr 18 Min Remaining

100%

Instructions Resources Help

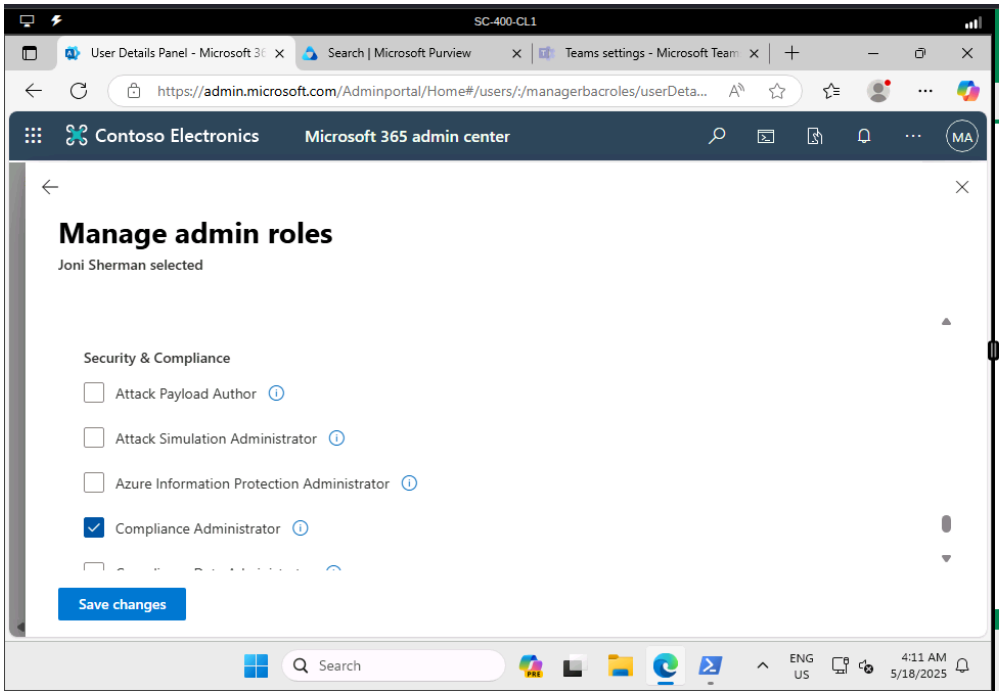
then select **Joni Sherman**.

5. The properties for Joni's account is displayed in a right, flyout panel. Select **Manage roles** on the flyout panel.
6. On the **Manage admin roles** panel, select the option for **Admin center access**, then scroll down to expand **Show all by category**.
7. Under the **Security & Compliance** category, select the checkbox for **Compliance Administrator**, then select **Save changes** at the bottom of the flyout panel.
8. You should receive a message stating **Admin roles updated**.
9. On the **Manage admin roles** page, select the **X** on the top right corner of the flyout panel to close the panel.
10. Sign out of the MOD Administrator account by selecting the **MA** icon in the top right, then select **Sign out**.



2% Tasks Complete

Previous Next



Microsoft Information Protection Administration

31 Hr 26 Min Remaining

100%

Instructions Resources Help

admin@WWLx097506.onmicrosoft.com

Admin's password should be provided by your lab hosting provider.

3. On the left sidebar, expand **Users** then select **Active users**.
4. On the **Active users** page, search for `Joni`, then select **Joni Sherman**.
5. The properties for Joni's account is displayed in a right, flyout panel. Select **Manage roles** on the flyout panel.
6. On the **Manage admin roles** panel, select the option for **Admin center access**, then scroll down to expand **Show all by category**.
7. Under the **Security & Compliance** category, select the checkbox for **Compliance Administrator**, then select **Save changes** at the bottom of the flyout panel.
8. You should receive a message stating **Admin roles updated**.
9. On the **Manage admin roles** page, select the **X** on the top right corner of the flyout panel to close the panel.

2% Tasks Complete

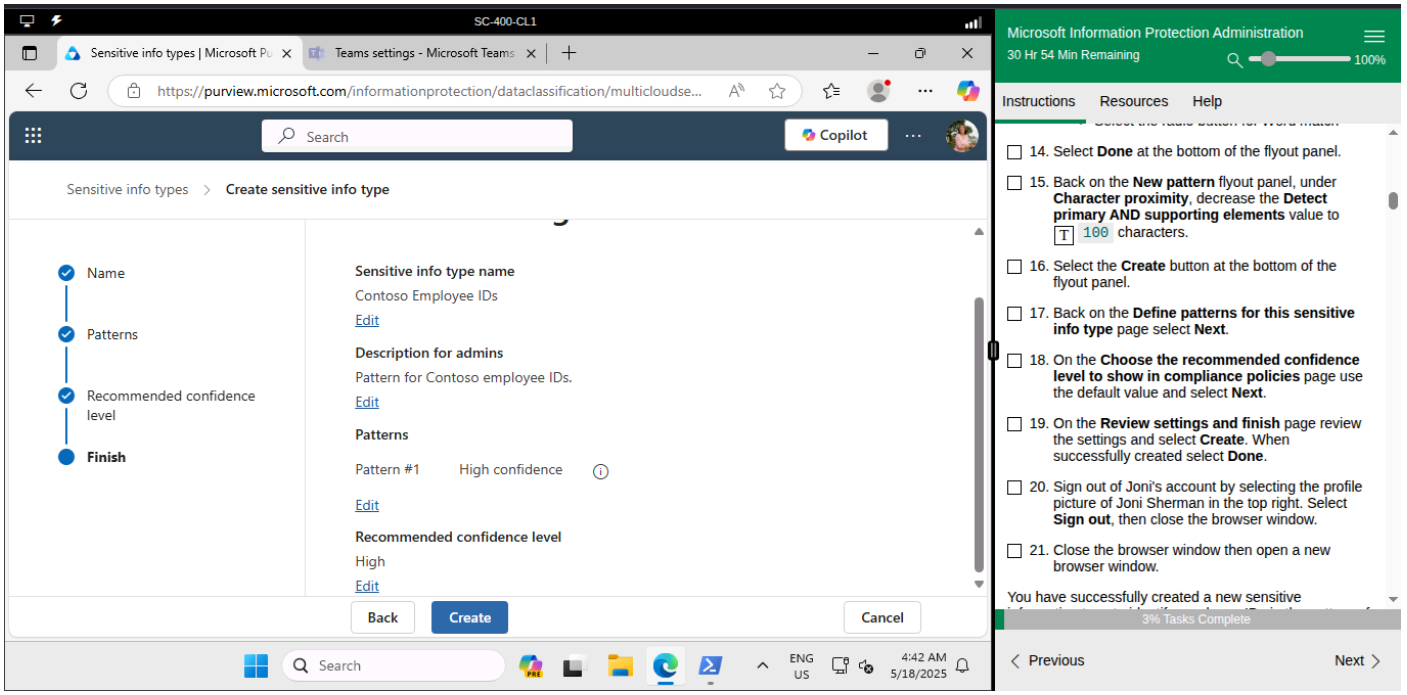
Previous Next

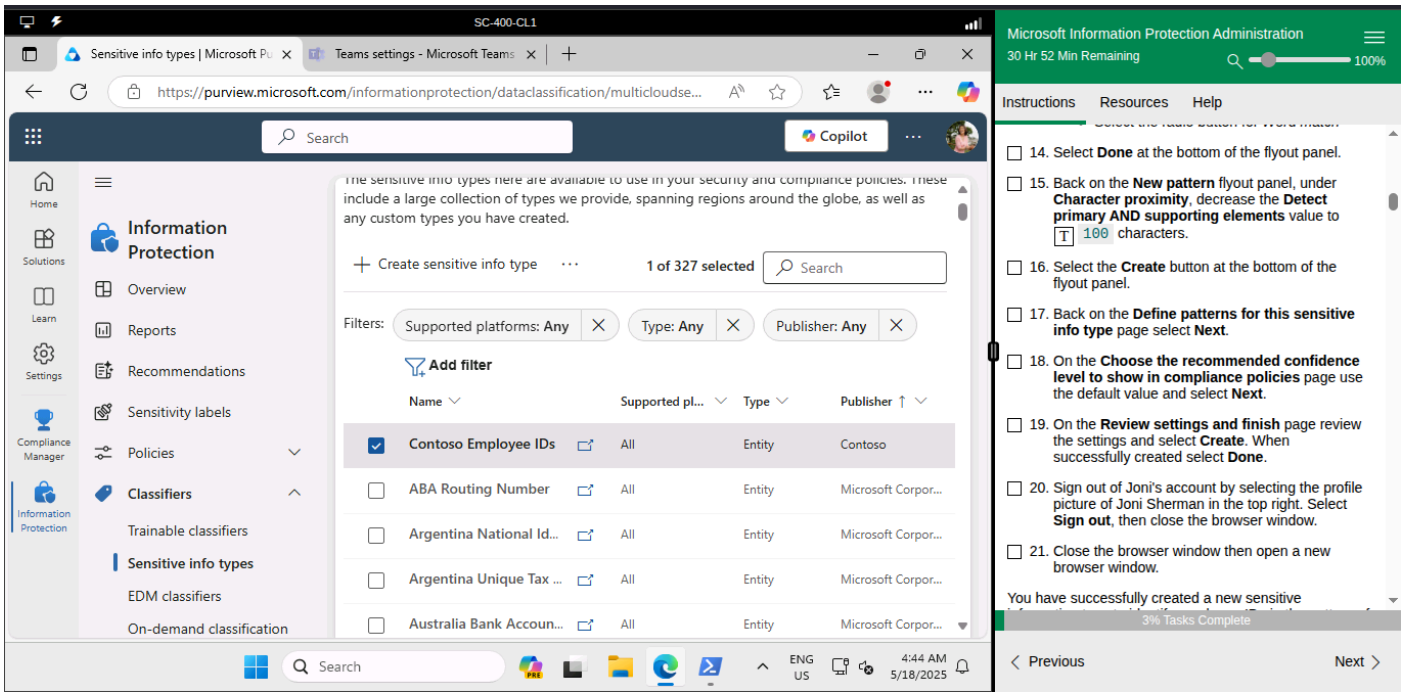
3. MANAGE SENSITIVE INFORMATION TYPES

Sensitive Information Types (SITs) are pattern-based data classifiers. They detect sensitive information like credit card numbers, invoice numbers or social security numbers. SITs are categorised into:

- Built-in SITs- these come with the Purview Portal by default and can be edited to create custom SITs
- Named entity SITs- these also come with Purview by default and detect names of people, physical addresses, and medical terms and conditions.
- Custom SITs- created by administrators to fit the needs of their organisations. They can be created by fully defining new SITs or modifying built-in SITs.
- Exact Data Match (EDM)- detects sensitive data by matching exact values from a defined secured database.

Below is a demonstration of creating custom SITs in the Microsoft Purview Portal.





Creation of EDM classifiers demonstration.