

# Microsoft

## Exam Questions SC-401

Administering Information Security in Microsoft 365



**NEW QUESTION 1**

- (Topic 1)

You need to meet the technical requirements for the creation of the sensitivity labels. To which user or users must you assign the Sensitivity Label Administrator role?

- A. Admin1 only
- B. Admin1 and Admin4 only
- C. Admin1 and Admin5 only
- D. Admin1, Admin2, and Admin3 only
- E. Admin1, Admin2, Admin4, and Admin5 only

**Answer:** D

**Explanation:**

To meet the requirement that all administrative users must be able to create Microsoft 365 sensitivity labels, we need to assign the Sensitivity Label Administrator role to the correct users.

Sensitivity Label Administrator Role Responsibilities

This role allows users to:

Create and manage sensitivity labels in Microsoft Purview. Publish and configure auto-labeling policies.

Modify label encryption and content marking settings.

Review of Admin Roles from the Table:

Admin	Role Assigned	Can Create Sensitivity Labels?
Admin1	Global Reader	<input type="checkbox"/> No, read-only permissions.
Admin2	Compliance Data Administrator	<input type="checkbox"/> Yes, can manage compliance data, including labels.
Admin3	Compliance Administrator	<input type="checkbox"/> Yes, has full compliance management, including labels.
Admin4	Security Operator	<input type="checkbox"/> No, this role is focused on security alerts and response.
Admin5	Security Administrator	<input type="checkbox"/> No, primarily focused on security policies and threat management.

Users that must be assigned the Sensitivity Label Administrator role: Admin2 (Compliance Data Administrator)  
 Admin3 (Compliance Administrator)  
 Admin1 (Global Reader) (should be assigned this role to fulfill the requirement that all admins can create labels).

**NEW QUESTION 2**

HOTSPOT - (Topic 1)

You are reviewing policies for the SharePoint Online environment.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
If a user creates a file in Site4 on January 1, 2021, users will be able to access the file on January 15, 2023.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2023.	<input type="checkbox"/>	<input type="checkbox"/>
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2026.	<input type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

AI-generated content may be incorrect. Understanding Site4's Retention Policies:

Site4RetentionPolicy1 deletes items older than 2 years from creation. If a file was created on January 1, 2021, it would be deleted after January 1, 2023.

Site4RetentionPolicy2 retains files for 4 years from creation. If a file was created on January 1, 2021, it will be kept until January 1, 2025, but not deleted after that (policy states "Do nothing").

Statement 1 - Yes, because Site4RetentionPolicy2 ensures files are retained for 4 years. Statement 2 - Yes, because Site4RetentionPolicy2 retains the file for 4 years (until January 1, 2025).

Statement 3 - No, because retention is only for 4 years (until January 1, 2025). After that, the policy does "nothing," meaning the file is no longer recoverable after that period.

**NEW QUESTION 3**

HOTSPOT - (Topic 1)

How many files in Site2 can User1 and User2 access after you turn on DLPpolicy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Number of files that User1 can access:

	▼
1	
2	
3	
4	

Number of files that User2 can access:

	▼
1	
2	
3	
4	

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Understanding DLP Policy Impact on File Access

The DLP policy (DLPpolicy1) applies to Site2 and restricts access when: Content contains SWIFT Codes.

Instance count is 2 or more.

File Analysis (Based on SWIFT Codes Count)

File Name	SWIFT Codes Count	DLP Policy Restricts Access?
File1.docx	1	<input type="checkbox"/> No restriction (SWIFT codes < 2)
File2.bmp	4	<input type="checkbox"/> Restricted (SWIFT codes ≥ 2)
File3.txt	3	<input type="checkbox"/> Restricted (SWIFT codes ≥ 2)
File4.xlsx	7	<input type="checkbox"/> Restricted (SWIFT codes ≥ 2)

Files that remain accessible (not restricted by DLP):

File1.docx (Contains only 1 SWIFT Code Below restriction threshold) User access after DLP policy is applied:

User	Role in Site2	Access Rights	Can Access Files?
User1	Site Owner	Full Access	File1.docx, plus override access to another file
User2	Site Visitor	Read-only	File1.docx only

User1 (Site Owner):

Has higher privileges and can override DLP restrictions (through admin intervention). Can access 2 files (File1.docx + override access to another file).

User2 (Site Visitor):

Has read-only access but DLP blocks access to restricted files. Can only access 1 file (File1.docx), since all others are restricted.

**NEW QUESTION 4**

HOTSPOT - (Topic 1)

You need to meet the technical requirements for the confidential documents.

What should you create first, and what should you use for the detection method? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Create first:

▼

A Compliance Manager assessment

A content search

A DLP policy

A sensitive info type

A sensitivity label

Use for detection method:

▼

Dictionary

File type

Keywords

Regular expression

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

To detect and protect confidential documents, we need a custom rule to identify project codes that start with 999 (since they are classified as confidential).

Box 1: A Sensitive Info Type (SIT) allows Microsoft Purview DLP policies to recognize structured data (e.g., project codes). DLP policies require a sensitive info

type to detect content based on patterns, keywords, or dictionary terms. A sensitivity label alone does not define detection logic—it is used for classification and protection after content is identified.

Box 2: Since project codes follow a structured 10-digit pattern, we should use a Regular Expression (Regex) to match project codes that start with 999.

Example Regex pattern: 999\d{7}

This pattern detects a 10-digit number starting with "999".

**NEW QUESTION 5**

- (Topic 2)

You have a Microsoft 365 E5 tenant that has devices onboarded to Microsoft Defender for Endpoint as shown in the following table.

Name	Type
Device1	Windows 11
Device2	Windows 10
Device3	iOS
Device4	macOS

You plan to start using Microsoft 365 Endpoint data loss protection (Endpoint DLP). Which devices support Endpoint DLP?

- A. Device1 only
- B. Device1 and Device2 only
- C. Device1 and Device4 only
- D. Device1, Device2, and Device4 only
- E. Device1, Device2, Device3, and Device4

**Answer: B**

**Explanation:**

Microsoft 365 Endpoint data loss prevention (Endpoint DLP) is supported only on Windows 10 and Windows 11 devices. It does not support macOS or iOS at this time.

From the provided table:

Device1 (Windows 11) - Supported Device2 (Windows 10) - Supported Device3 (iOS) - Not supported Device4 (macOS) - Not supported

Thus, only Device1 and Device2 support Endpoint DLP.

**NEW QUESTION 6**

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role group
Admin1	Insider Risk Management Admins
Admin2	Insider Risk Management Analysts
Admin3	Risk Management Investigators
Admin4	Insider Risk Management Auditors

You plan to create a Microsoft Purview insider risk management case named Case1. Which insider risk management object should you select first, and which users will be

added as contributors for Case1 by default?

To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

## Answer Area

Object:

An alert

A policy

A risky user

A notice template

Forensic evidence

Users:

Admin1 and Admin2 only

Admin2 and Admin3 only

Admin3 and Admin4 only

Admin2, Admin3, and Admin4 only

Admin1, Admin2, Admin3, and Admin4

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: When creating a Microsoft Purview Insider Risk Management case, you must first select a risky user to investigate. The case will be built around this specific user's activities, linking alerts and risk signals to the investigation.

Box 2: The Insider Risk Management role groups determine who can access and contribute to cases:

Admin1 (Insider Risk Management Admins) Full admin access.

Admin2 (Insider Risk Management Analysts) Analysts who review cases. Admin3 (Risk Management Investigators) Investigators who work on cases. Admin4 (Insider Risk Management Auditors) Auditors who oversee cases.

All these roles have default access to insider risk cases in Microsoft Purview, so all four admins are added as contributors.

**NEW QUESTION 7**

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription.

You need to implement a compliance solution that meets the following requirements:

Captures clips of key security-related user activities, such as the exfiltration of sensitive company data.

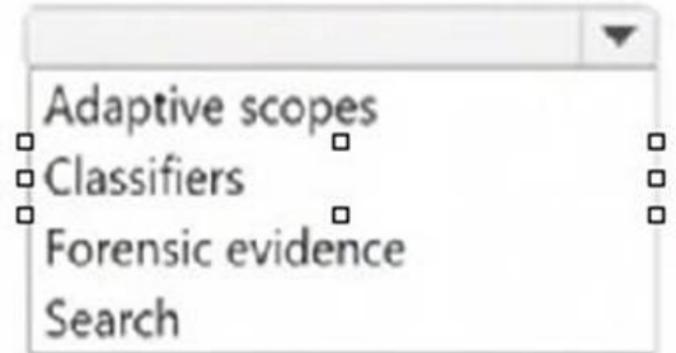
Integrates data loss prevention (DLP) capabilities with insider risk management.

What should you use for each requirement? To answer, select the appropriate options in the answer area.

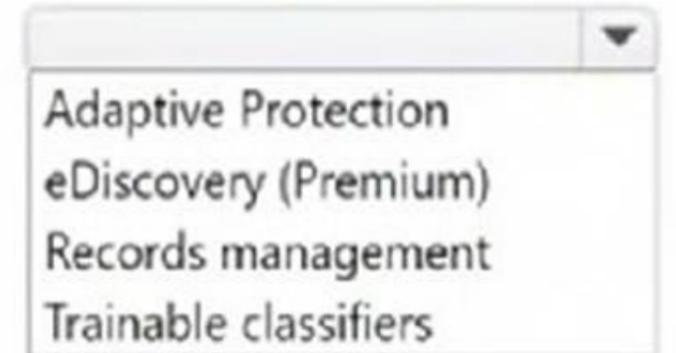
NOTE: Each correct selection is worth one point.

### Answer Area

Captures clips of key security-related user activities:



Integrates DLP capabilities with insider risk management:



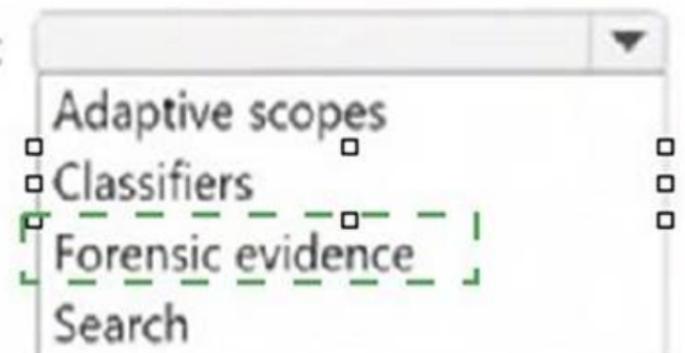
- A. Mastered
- B. Not Mastered

Answer: A

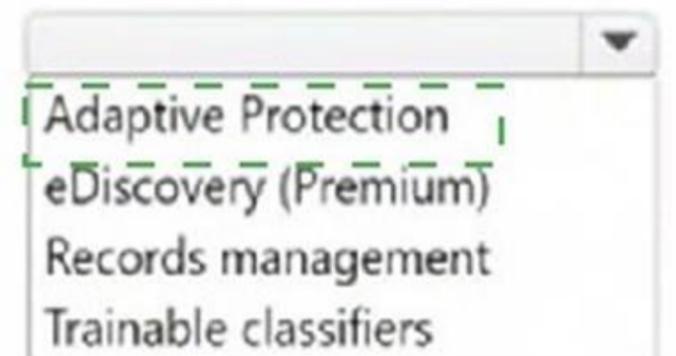
Explanation:

### Answer Area

Captures clips of key security-related user activities:



Integrates DLP capabilities with insider risk management:



#### NEW QUESTION 8

- (Topic 2)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You have a user named User1. Several users have full access to the mailbox of User1. Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in the Microsoft Purview portal to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1. Solution: You run the Set-Mailbox -Identity "User1" -AuditEnabled \$true command. Does that meet the goal?

- A. Yes
- B. No

Answer: A

**Explanation:**

To track who accesses User1's mailbox, you need to enable mailbox auditing for User1. By default, Exchange mailbox auditing is not enabled per mailbox (even though it is enabled tenant-wide).

The Set-Mailbox -Identity "User1" -AuditEnabled \$true command enables audit logging for mailbox actions like:

Read emails Delete emails

Send emails as User1 Access by delegated users

Once enabled, you can search for future sign-ins and actions in the Microsoft Purview audit logs.

**NEW QUESTION 9**

DRAG DROP - (Topic 2)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.

You plan to deploy a Defender for Cloud Apps file policy that will be triggered when the following conditions are met:

A file is shared externally.

A file is labeled as internal only.

Which filter should you use for each condition? To answer, drag the appropriate filters to the correct conditions. Each filter may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

**Filters**

0 Access level

0 Collaborators

0 Matched policy

0 Sensitivity label

**Answer Area**

When a file is shared externally.

When a file is labelled as Internal only.

**Filter**

0

0

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Filters**

0 Access level

0 Collaborators

0 Matched policy

0 Sensitivity label

**Answer Area**

When a file is shared externally.

When a file is labelled as Internal only.

**Filter**

0 Access level

0 Sensitivity label

**NEW QUESTION 10**

- (Topic 2)

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Description
User1	<ul style="list-style-type: none"> <li>User 1 is a regional manager.</li> <li>User1 is assigned the Reader role.</li> <li>Three department managers report to User1.</li> </ul>
User2	<ul style="list-style-type: none"> <li>User2 is the human resources (HR) department manager.</li> <li>User2 has no Microsoft Entra roles assigned.</li> <li>Five HR department users report to User2.</li> </ul>
User3	<ul style="list-style-type: none"> <li>User3 is a developer.</li> <li>User3 reports to User2.</li> <li>User3 is the only user in the compliance department.</li> <li>User3 is assigned the Compliance Administrator role.</li> </ul>
User4	<ul style="list-style-type: none"> <li>User4 is the assistant of User1.</li> <li>User4 has no Microsoft Entra roles assigned.</li> <li>User4 handles a high volume of confidential data on behalf of User1.</li> </ul>

Which users will Microsoft Purview insider risk management flag as potential high-impact users?

- A. User1 and User2 only
- B. User2 and User3 only
- C. User1, User2, and User3 only
- D. User1, User2, User3, and User4

**Answer:** D

**Explanation:**

Microsoft Purview Insider Risk Management flags high-impact users based on various risk factors, including role, access to confidential data, and influence within an organization. Let's analyze each user:

User1 (Regional Manager, assigned Reader role, manages department managers) Risk Factors:

Holds a managerial position (regional manager).

Manages multiple department managers, indicating organizational influence. Access to critical business information.

Flagged? -Yes (Managerial role and access to confidential data).

User2 (HR department manager, no Microsoft Entra roles, manages HR department users) Risk Factors:

Manages HR department users, meaning they likely handle sensitive employee data. HR roles are often considered high-risk due to access to personal and payroll data.

Flagged? -Yes (HR role and access to sensitive employee data).

User3 (Developer, reports to User2, only user in compliance, assigned Compliance Administrator role)

Risk Factors:

Compliance Administrator role grants access to sensitive security and regulatory data. Only person in the compliance department, meaning they hold a critical role.

Potentially high impact on compliance and security settings.

Flagged? -Yes (Privileged Compliance Administrator role).

User4 (Assistant to User1, no Entra roles, handles confidential data on behalf of User1)

Risk Factors:

Handles a high volume of confidential data on behalf of a regional manager. Assistants with access to sensitive data are considered insider risk candidates.

Flagged? -Yes (High access to sensitive information).

Since all four users fit high-impact criteria (managerial roles, privileged compliance access, handling sensitive data), Microsoft Purview Insider Risk Management will flag all of them.

**NEW QUESTION 10**

- (Topic 2)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You have a user named User1. Several users have full access to the mailbox of User1. Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in the Microsoft Purview portal to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1. Solution: You run the Set-MailboxFolderPermission -Identity "User1" -User User1@contoso.com -AccessRights Owner command.

Does that meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

The Set-MailboxFolderPermission -Identity "User1" -User User1@contoso.com - AccessRights Owner command is incorrect. This assigns folder permissions but does not enable auditing. It does not track who accessed the mailbox or deleted emails.

**NEW QUESTION 15**

- (Topic 2)

You have a Microsoft 365 E5 subscription.

You need to review a Microsoft 365 Copilot usage report. From where should you review the report?

- A. Information Protection in the Microsoft Purview portal
- B. the Microsoft 365 admin center
- C. DSPM for AI in the Microsoft Purview portal
- D. the Microsoft Defender portal

**Answer:** C

**Explanation:**

To review a Microsoft 365 Copilot usage report, you need to use Data Security Posture Management for AI (DSPM for AI) in the Microsoft Purview portal. DSPM for AI provides insights into AI-related activities, including Copilot usage, risk assessments, and data security posture related to AI interactions within Microsoft 365.

**NEW QUESTION 16**

DRAG DROP - (Topic 2)

You have a Microsoft 365 subscription that contains 20 data loss prevention (DLP) policies. You need to identify the following:

Rules that are applied without triggering a policy alert  
 The top 10 files that have matched DLP policies  
 Alerts that are miscategorized

Which report should you use for each requirement? To answer, drag the appropriate reports to the correct requirements. Each report may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Reports	Answer Area	Report
DLP policy matches	Rules that are applied without triggering a policy alert:	<input type="text"/>
False positive and override	The top 10 files that have matched DLP policies:	<input type="text"/>
Incident reports	Alerts that are miscategorized:	<input type="text"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

The False positive and override report helps identify rules that were applied but did not generate an actual policy alert, which means they were overridden or deemed false positives.

The DLP policy matches report provides details on files that matched DLP policies, including the top 10 files.

The Incident reports report helps analyze and review alerts, including those that may have been miscategorized.

**NEW QUESTION 18**

- (Topic 2)

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.

You need to implement Microsoft Purview data lifecycle management. What should you create first?

- A. a sensitivity label policy
- B. a data loss prevention (DLP) policy
- C. an auto-labeling policy
- D. a retention label

**Answer:** D

**Explanation:**

To implement Microsoft Purview Data Lifecycle Management for SharePoint Online (Site1), you need to create a retention label first. Retention labels define how long content should be retained or deleted based on compliance requirements. Once a retention label is created, it can be manually or automatically applied to content in SharePoint Online, Exchange, OneDrive, and Teams. After creating a retention label, you can configure label policies to apply them to Site1 and other locations.

**NEW QUESTION 20**

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription that contains a user named User1.

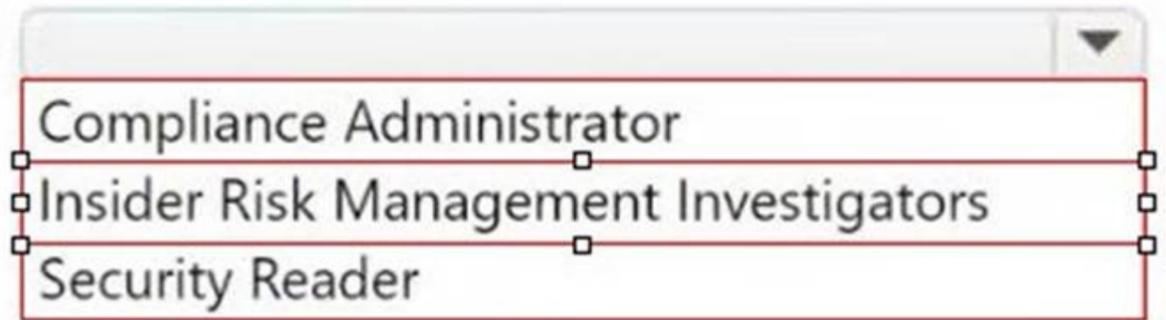
You deploy Microsoft Purview Data Security Posture Management for AI (DSPM for AI). You need to ensure that User1 can perform the following actions:  
 View recommendations from the Recommendations page. View the user risk level for all events by using Activity explorer. The solution must follow the principle of least privilege.

To which role group should you add User1 for each action? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

View the recommendations:



A screenshot of a dropdown menu with a downward arrow in the top right corner. The menu is open, showing three options: 'Compliance Administrator', 'Insider Risk Management Investigators', and 'Security Reader'. Each option has a small square selection box to its left.

View the user risk level:



A screenshot of a dropdown menu with a downward arrow in the top right corner. The menu is open, showing four options: 'Compliance Administrator', 'Insider Risk Management Analysts', 'Insider Risk Management Investigators', and 'Security Reader'. Each option has a small square selection box to its left.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: The Insider Risk Management Investigators role allows users to view recommendations related to insider risk cases and Microsoft Purview DSPM for AI insights. This role is appropriate because it grants access to review AI-related risk recommendations without unnecessary administrative privileges.

Box 2: The Insider Risk Management Analysts role allows users to analyze user risk levels and events using Activity Explorer. This follows the principle of least privilege, ensuring that User1 can only view risk levels and investigate but does not gain full administrative control over insider risk policies.

**NEW QUESTION 21**

- (Topic 2)

You have a Microsoft 365 subscription.

You need to customize encrypted email for the subscription. The solution must meet the following requirements.

Ensure that when an encrypted email is sent, the email includes the company logo. Minimize administrative effort.

Which PowerShell cmdlet should you run?

- A. Set-IRMConfiguration
- B. Set-OMEConfiguration
- C. Set-RMSTemplate
- D. New-OMEConfiguration

**Answer:** B

**Explanation:**

To customize encrypted email in Microsoft 365, including adding a company logo, you need to modify the Office Message Encryption (OME) branding settings. The Set-OMEConfiguration PowerShell cmdlet allows you to configure branding elements such as: Company logo

Custom text Background color

This cmdlet is used to update existing OME branding settings, ensuring that encrypted emails sent from your organization include the required customizations.

**NEW QUESTION 24**

- (Topic 2)

You have a Microsoft 365 E5 subscription that contains a retention policy named RP1 as shown in the following table.

Setting	Value
Location	<ul style="list-style-type: none"> <li>• Exchange email (All recipients)</li> <li>• SharePoint sites (All sites)</li> </ul>
Retain items for a specific period	5 years (When items were created)
At the end of the retention period	Delete items automatically

You place a preservation lock on RP1. You need to modify RP1.

Which two modifications can you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add locations to the policy.
- B. Delete the policy.
- C. Remove locations from the policy.
- D. Decrease the retention period of the policy.
- E. Disable the policy.
- F. Increase the retention period of the policy.

**Answer:** AF

**Explanation:**

A Preservation Lock in Microsoft Purview Retention Policies enforces strict compliance and prevents certain modifications to ensure data is retained according to compliance requirements.

When a Preservation Lock is applied:

- \* 1. You cannot disable or delete the policy.
- \* 2. You cannot remove locations from the policy.
- \* 3. You cannot decrease the retention period.
- \* 4. You can add locations to the policy.
- \* 5. You can increase the retention period.

You can expand the retention policy to cover additional locations (e.g., more Exchange mailboxes, SharePoint sites). You can extend the retention duration (e.g., increase from 5 years to 10 years) since this aligns with stricter compliance.

**NEW QUESTION 29**

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription that has data loss prevention (DLP) implemented.

You plan to export DLP activity by using Activity explorer.

The exported file needs to display the sensitive info type detected for each DLP rule match. What should you do in Activity explorer before exporting the data, and in which file format is the file exported? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

## Answer Area

In Activity explorer:

▼

Add a custom column

Apply a built-in filter

Customize the default filter

File type:

▼

CSV

JSON

TXT

XML

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: To include the sensitive info type detected for each DLP rule match, you need to add a custom column in Activity Explorer. This ensures that the exported file contains specific details about the detected sensitive information types.

Box 2: DLP activity exports from Activity Explorer are always in CSV (Comma-Separated Values) format. This format allows for easy data analysis and reporting in Excel or other data-processing tools.

**NEW QUESTION 32**

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription that uses Microsoft Purview.

You need ensure that an incident will be generated when a user visits a phishing website. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

Type of policy to create:

▼

- a Communication compliance
- a Data loss prevention (DLP)
- an Insider risk management

Prerequisite to complete:

▼

- Create a sensitive service domain group.
- Deploy the Microsoft Defender Browser Protection extension.
- Deploy the Microsoft Purview extension.
- From Data Loss Prevention, configure the Service domains settings.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Insider Risk Management policies in Microsoft Purview can be configured to detect risky behavior, such as accessing phishing websites. These policies monitor user activity, generate alerts, and help organizations investigate potential security threats.  
 Box 2: Microsoft Defender Browser Protection extension helps in detecting unsafe or phishing websites and integrating this detection with Insider Risk Management policies. This extension works with Microsoft Edge and Google Chrome to identify risky browsing activity and trigger alerts.

**NEW QUESTION 33**

- (Topic 2)

You have a Microsoft 365 E5 subscription.

You need to create a sensitivity label named Label1. The solution must ensure that users can use Microsoft 365 Copilot to summarize files that have Label1 applied.

Which permission should you select for Label1?

- A. Export content(EXPORT)
- B. Copy and extract content(EXTRACT)
- C. Edit content(DOCEDIT)
- D. View rights(VIEW)

**Answer:** B

**Explanation:**

To allow Microsoft 365 Copilot to summarize files that have Label1 applied, the label must grant permission to extract content from the document. The correct permission for this is Copy and extract content (EXTRACT).  
 Microsoft 365 Copilot requires access to read and process content in documents to generate summaries. The EXTRACT permission allows users (and AI tools like Copilot) to copy and extract content for processing while still maintaining the protection applied by the sensitivity label.

**NEW QUESTION 37**

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription. The subscription contains devices that are onboarded to Microsoft Purview and configured as shown in the following table.

Name	Operating system	Microsoft Purview browser extension
Device1	Windows 11	Installed
Device2	Windows 11	Not installed
Deivce3	macOS	Installed

The subscription contains the users shown in the following table.

Name	Activity performed during the last seven days	On device
User1	Used a generative AI website to generate an image	Device1
User2	Asked Microsoft 365 Copilot to summarize a document	Device2
User3	Browsed sample content on a generative AI website	Device3

You need to review the activities.

What should you use for each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

User1:  Activity explorer in Data Security Posture Management for AI (DSPM for AI)  
 Audit log search  
 Insider risk audit log  
 Unified Catalog

User2: Activity explorer in Data Security Posture Management for AI (DSPM for AI)  
 Audit log search  
 Insider risk audit log  
 Unified Catalog

User3: Activity explorer in Data Security Posture Management for AI (DSPM for AI)  
 Audit log search  
 Insider risk audit log  
 Unified Catalog

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

User1: Since the Microsoft Purview browser extension is installed on Device1, AI-related activity performed by User1 (generating an image using a generative AI website) can be reviewed in Activity explorer in DSPM for AI.  
 User2: Since Device2 does not have the Microsoft Purview browser extension installed, AI-related activity cannot be tracked in DSPM for AI. Instead, Audit log search should be used to review activity such as using Microsoft 365 Copilot.  
 User3: Since Device3 has the Microsoft Purview browser extension installed, AI-related activity (browsing sample content on a generative AI website) can be reviewed using Activity explorer in DSPM for AI.

**NEW QUESTION 39**

- (Topic 2)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You recently discovered that the developers at your company emailed Azure Storage Account keys in plain text to third parties.

You need to ensure that when Azure Storage Account keys are emailed, the emails are encrypted.

Solution: You create a data loss prevention (DLP) policy that has only the Exchange email location selected.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

**Explanation:**

To ensure Azure Storage Account keys are encrypted when sent via email, you need a Data Loss Prevention (DLP) policy that detects Azure Storage Account keys using a sensitive information type and automatically encrypts emails containing these keys.

A DLP policy with Exchange email as the only location meets this requirement because it identifies sensitive data in email messages and it applies protection actions, such as encryption, blocking, or alerts.

**NEW QUESTION 43**

- (Topic 2)

You have a Microsoft 365 E5 subscription.

You need to create static retention policies for the following locations:

Teams chats Exchange email SharePoint sites Microsoft 365 Groups

Teams channel messages

What is the minimum number of retention policies required?

- A. 1
- B. 2
- C. 3

- D. 4
- E. 5

**Answer: C**

**Explanation:**

In Microsoft Purview Data Lifecycle Management, different Microsoft 365 locations require separate retention policies because they fall under different storage and compliance models.

Teams Chats & Teams Channel Messages (1 Policy) require a separate retention policy because Teams messages are stored differently than Exchange and SharePoint content. One policy can cover both Teams chats and Teams channel messages. Exchange Email (1 Policy) requires its own separate policy since emails are managed differently than Teams or SharePoint content. SharePoint Sites & Microsoft 365 Groups (1 Policy) are both stored in SharePoint Online, so they can be managed under one policy.

**NEW QUESTION 45**

- (Topic 2)

You have Microsoft 365 E5 subscription.

You create two alert policies named Policy1 and Policy2 that will be triggered at the times shown in the following table.

Policy	Time (hh:mm:ss)
Policy1	10:00:00
Policy2	10:00:03
Policy1	10:00:04
Policy2	10:00:31
Policy1	10:01:01
Policy1	10:04:45

How many alerts will be added to the Microsoft Purview portal?

- A. 2
- B. 3
- C. 4
- D. 5
- E. 6

**Answer: D**

**Explanation:**

In Microsoft Purview, when multiple alert policies trigger alerts, duplicate alerts within a short period (typically 5 minutes) may be suppressed to avoid redundancy. Step-by-step Analysis:

Policy	Time Triggered (hh:mm:ss)	New Alert?
Policy1	10:00:00	Yes
Policy2	10:00:03	Yes
Policy1	10:00:04	No (Duplicate within 5 min)
Policy2	10:00:31	No (Duplicate within 5 min)
Policy1	10:01:01	Yes
Policy1	10:04:45	Yes

Policy1 at 10:00:04 is ignored because Policy1 already triggered at 10:00:00, and it's within 5 minutes.

Policy2 at 10:00:31 is ignored because Policy2 already triggered at 10:00:03, and it's within 5 minutes.

Policy1 at 10:01:01 is a new alert because it's over 1 minute after the previous Policy1 alert.

Policy1 at 10:04:45 is a new alert because it's over 3 minutes after the previous Policy1 alert.

**NEW QUESTION 49**

- (Topic 2)

You are planning a data loss prevention (DLP) solution that will apply to Windows Client computers.

You need to ensure that when users attempt to copy a file that contains sensitive information to a USB storage device, the following requirements are met:

If the users are members of a group named Group1, the users must be allowed to copy the file, and an event must be recorded in the audit log.

All other users must be blocked from copying the file. What should you create?

- A. one DLP policy that contains one DLP rule
- B. one DLP policy that contains two DLP rules
- C. two DLP policies that each contains one DLP rule

**Answer: B**

**Explanation:**

To meet the requirements, you need one DLP policy with two separate DLP rules to handle the different conditions:

\* 1. First DLP Rule (For Group1 Members): If the user is a member of Group1 and attempts to copy a file with sensitive data to a USB storage device. Allow the file copy but log the event in the audit log.

\* 2. Second DLP Rule (For All Other Users): If any user who is NOT in Group1 attempts to copy a file with sensitive data to a USB storage device. Block the file transfer.

**NEW QUESTION 50**

- (Topic 2)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You have a user named User1. Several users have full access to the mailbox of User1. Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in the Microsoft Purview portal to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1. Solution: You run the Set-AdminAuditLogConfig -AdminAuditLogEnabled \$true -AdminAuditLogCmdlets \*Mailbox\* command. Does that meet the goal?

- A. Yes
- B. No

**Answer: B**

**Explanation:**

The Set-AdminAuditLogConfig -AdminAuditLogEnabled \$true -AdminAuditLogCmdlets

\*Mailbox\* command is incorrect. This enables admin audit logging, which tracks changes to mailbox configurations (e.g., mailbox settings updates), not user activity inside the mailbox.

**NEW QUESTION 54**

- (Topic 2)

You have a Microsoft 365 subscription.

You need to ensure that users can apply retention labels to individual documents in their Microsoft SharePoint libraries.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. From Microsoft Defender for Cloud Apps, create a file policy.
- B. From the SharePoint admin center, modify the Site Settings.
- C. From the SharePoint admin center, modify the records management settings.
- D. From the Microsoft Purview portal, publish a label.
- E. From the Microsoft Purview portal, create a label.

**Answer: DE**

**Explanation:**

To allow users to apply retention labels to individual documents in Microsoft SharePoint libraries, you need to create a retention label and publish the label.

In Microsoft Purview, retention labels define how long content should be retained or deleted. You must first create a label that specifies the retention rules. After creating the label, you must publish it so that it becomes available for users in SharePoint document libraries. Once published, users can manually apply the retention label to individual documents.

**NEW QUESTION 57**

- (Topic 2)

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft Purview insider risk management. You implement the HR data connector.

You need to prepare the data that will be imported by the data connector. In which format should you prepare the data?

- A. JSON
- B. CSV
- C. TSV
- D. XML
- E. PRN

**Answer: B**

**Explanation:**

When implementing Microsoft Purview Insider Risk Management and using the HR data connector, you must prepare HR data in CSV (Comma-Separated Values) format. This format is required because Microsoft Purview supports CSV files for importing user employment details, termination dates, role changes, and other HR-related attributes.

**NEW QUESTION 61**

- (Topic 2)

You need to be alerted when users share sensitive documents from Microsoft OneDrive to any users outside your company. What should you do?

- A. From the Microsoft Purview portal create an insider risk policy
- B. From the Microsoft Defender portal create a file policy
- C. From the Microsoft Defender portal, create an activity policy.
- D. From the Microsoft Purview portal, start a data investigation.

**Answer: B**

**Explanation:**

An activity policy in Microsoft Defender for Cloud Apps (Microsoft Defender portal) allows you to track and alert on specific user actions, such as sharing sensitive documents externally from OneDrive. This policy can detect file-sharing activities and send alerts when files are shared with external users, which meets the requirement.

**NEW QUESTION 65**

- (Topic 2)

You have a Microsoft 365 E5 subscription.

You plan to implement insider risk management for users that manage sensitive data associated with a project.

You need to create a protection policy for the users. The solution must meet the following requirements:

Minimize the impact on users who are NOT part of the project. Minimize administrative effort.

What should you do first?

- A. From the Microsoft Purview portal, create an insider risk management policy.
- B. From the Microsoft Entra admin center, create a security group
- C. C From the Microsoft Entra admin center create a User risk policy D From the Microsoft Purview portal create a priority user group

**Answer: B**

**Explanation:**

To implement insider risk management for users managing sensitive project data while minimizing the impact on other users and reducing administrative effort, you should first create a security group in Microsoft Entra ID (formerly Azure AD).

Security groups allow you to scope insider risk management policies to specific users instead of applying policies to all users, which helps in minimizing unnecessary alerts and reducing administrative overhead. After creating the security group, you can assign this group to a Microsoft Purview Insider Risk Management policy, ensuring that only project- related users are affected.

**NEW QUESTION 68**

HOTSPOT - (Topic 2)

You plan to create a custom sensitive information type that will use Exact Data Match (EDM).

You need to identify what to upload to Microsoft 365, and which tool to use for the upload. What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

Upload:

- Data hashes
- Data in the XML format
- Digitally signed data

Use:

- Azure Storage Explorer
- EDM upload agent
- Microsoft Purview portal
- The Set-DlpKeywordDictionary cmdlet

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

EDM does not store raw data; instead, it requires hashed versions of sensitive data for privacy and security. To upload the hashed data, Microsoft provides the EDM upload agent. This ensures that the data is securely processed and recognized by the EDM service in Microsoft 365.

**NEW QUESTION 70**

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### **SC-401 Practice Exam Features:**

- \* SC-401 Questions and Answers Updated Frequently
- \* SC-401 Practice Questions Verified by Expert Senior Certified Staff
- \* SC-401 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* SC-401 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SC-401 Practice Test Here](#)**