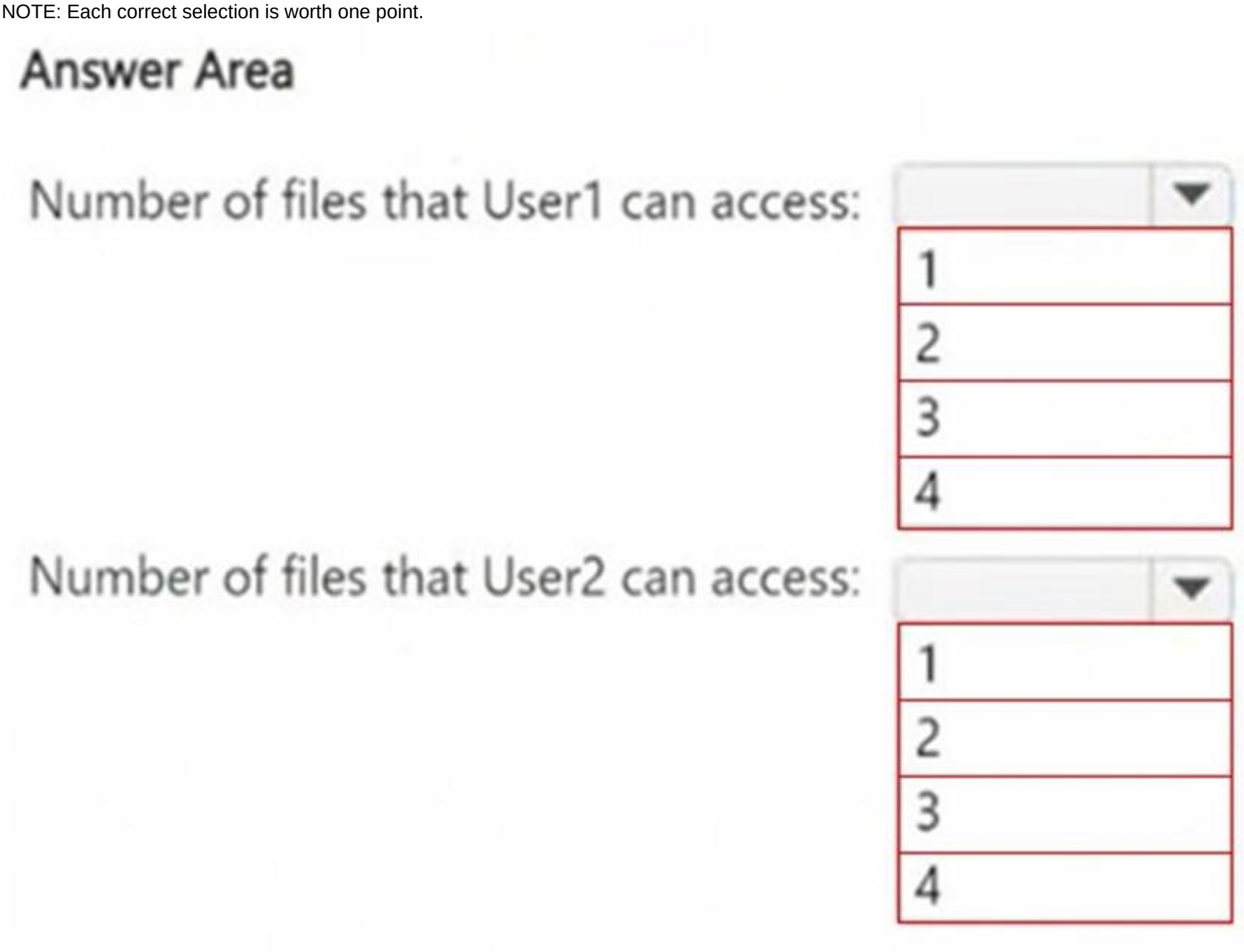
# Microsoft

## Exam Questions SC-401

Administering Information Security in Microsoft 365

**NEW QUESTION 1**
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.




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 | ☐ No restriction (SWIFT codes < 2) |
| File2.bmp | 4 | ☐ Restricted (SWIFT codes ≥ 2) |
| File3.txt | 3 | ☐ Restricted (SWIFT codes ≥ 2) |
| File4.xlsx | 7 | ☐ 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 2**
- (Topic 2)
You have a Microsoft 365 tenant.
You have a database that stores customer details. Each customer has a unique 13-digit identifier that consists of a fixed pattern of numbers and letters.
You need to implement a data loss prevention (DLP) solution that meets the following
requirements:
Email messages that contain a single customer identifier can be sent outside your company.
Email messages that contain two or more customer identifiers must be approved by the company's data privacy team.
Which two components should you include in the solution? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a sensitivity label
B. a sensitive information type
C. a DLP policy
D. a retention label
E. a mail flow rule

**Answer:** BC

**Explanation:**
You need to define a custom sensitive information type that recognizes the unique 13-digit identifier format for customer records. Microsoft Purview DLP policies use these types to identify and protect sensitive data.
A Data Loss Prevention (DLP) policy is required to enforce the rules. It will allow emails with a single identifier but trigger an approval workflow when two or more identifiers are detected.

**NEW QUESTION 3**
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.

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

**NEW QUESTION 4**
- (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 tenant and 500 computers that run Windows 11. The computers are onboarded to Microsoft Purview.
You discover that a third-party application named Tailspin_scanner.exe accessed protected sensitive information on multiple computers. Tailspin_scanner.exe is installed locally on the computers.
You need to block Tailspin_scanner.exe from accessing sensitive documents without preventing the application from accessing other documents.
Solution: From Microsoft Defender for Cloud Apps, you create an app discovery policy. Does this meet the goal?

A. Yes
B. No

**Answer:** B

**Explanation:**
Creating an app discovery policy in Microsoft Defender for Cloud Apps is used for detecting and monitoring cloud application usage, but it does not prevent a locally installed application (Tailspin_scanner.exe) from accessing sensitive files on Windows 11 devices.
To block Tailspin_scanner.exe from accessing sensitive documents while allowing it to access other files, the correct solution is to use Microsoft Purview Endpoint Data Loss Prevention (Endpoint DLP) and add Tailspin_scanner.exe to the Restricted Apps list.
Endpoint DLP allows you to block specific applications from accessing sensitive files while keeping general access available. Restricted Apps List in Endpoint DLP ensures that Tailspin_scanner.exe cannot open, copy, or process protected documents, but it can still function normally for non-sensitive content.

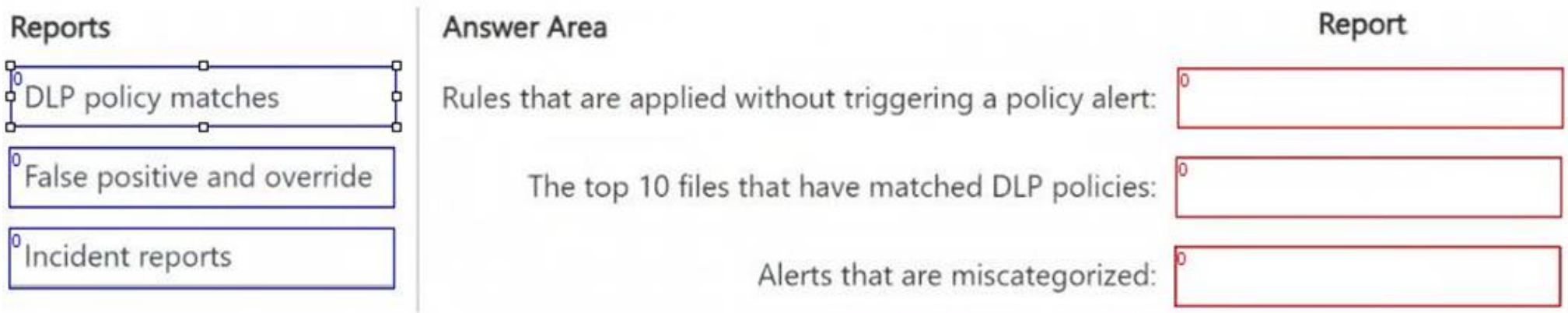
**NEW QUESTION 5**
- (Topic 2)
You have a Microsoft 365 E5 subscription.
You need to review a Microsoft 365 Copilot usage report. From where should you review the report?

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 6**
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.

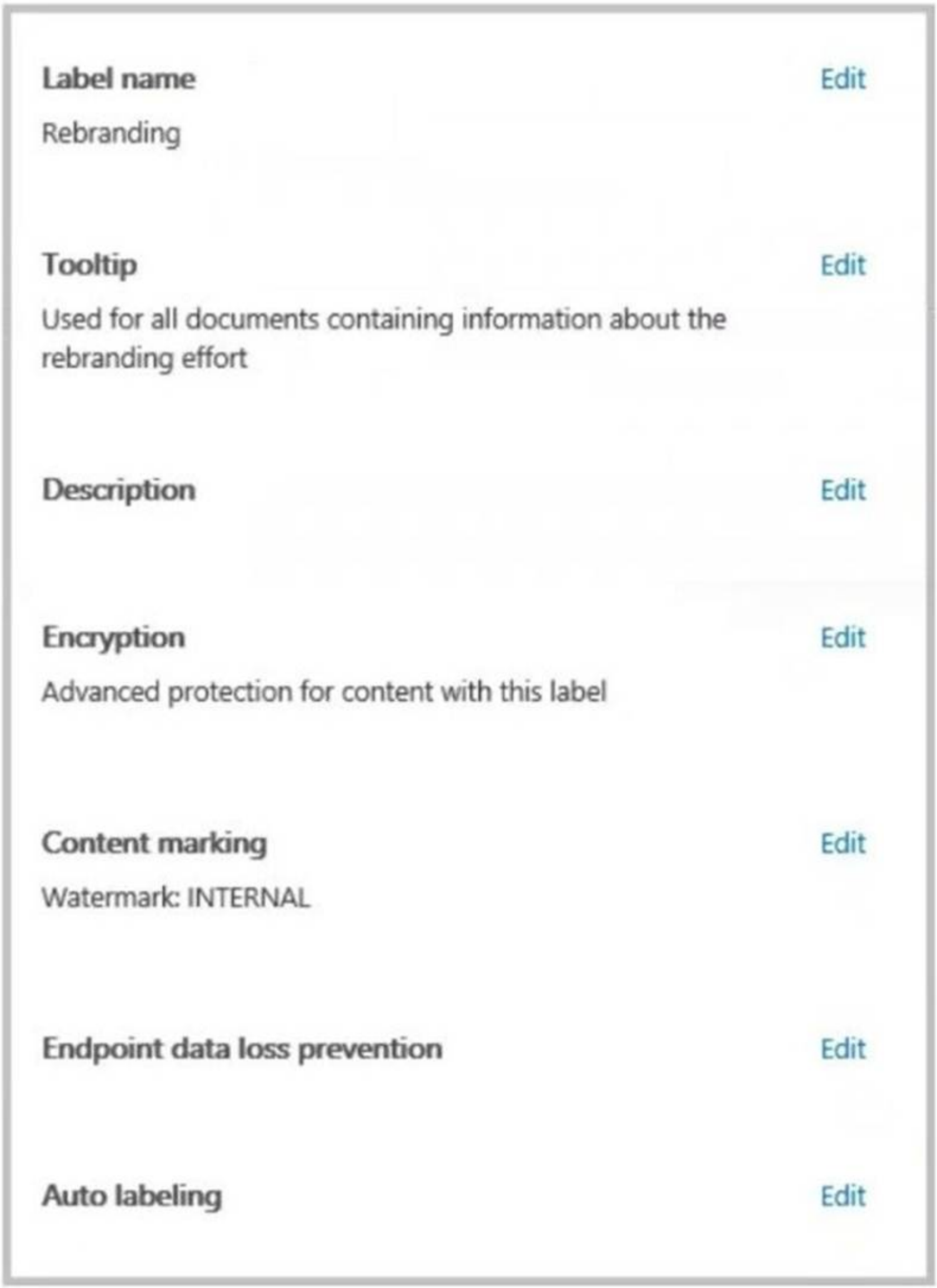



A. Mastered
B. Not Mastered

**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 7**
HOTSPOT - (Topic 2)
You have a Microsoft 365 sensitivity label that is published to all the users in your Microsoft Entra tenant as shown in the following exhibit.




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

Answer Area

| Statements | Yes | No |
|---|---|---|
| All the documents stored on each user's computer will include a watermark automatically. | ○ | ○ |
| If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL". | ○ | ○ |
| The sensitivity label can be applied only to documents that contain the word rebranding. | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Statement 1 - No. The sensitivity label includes content marking (watermark: INTERNAL), but it only applies to documents where the label is manually or automatically applied, not to all documents by default.
Statement 2 - No. The sensitivity label only specifies a watermark, not a header. If a header marking was configured, it would explicitly appear in the label settings.
Statement 3 - No. There is no indication that auto-labeling is configured to apply the label only to documents with the word "rebranding". Auto-labeling is an optional setting that needs explicit configuration.

**NEW QUESTION 8**
HOTSPOT - (Topic 2)
You have a Microsoft 365 E5 subscription.
You need to identify documents that contain patent application numbers containing the letters PA followed by eight digits, for example, PA 12345678. The solution must minimize administrative effort.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

To identify the documents, use a data classification of:
- Exact data match (EDM)
- Sensitive info type
- Trainable classifier

Configure data classifications by using a:
- Keyword dictionary
- Regular expression
- Function

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Box 1: Since you are looking for a specific pattern (PA followed by eight digits, e.g., PA 12345678), the best classification method is Sensitive Info Type. Sensitive Info Types allow pattern-based matching to identify structured data. Exact Data Match (EDM) is not needed because you're not comparing against a fixed dataset. Trainable classifier is not appropriate because this is a structured pattern, not an unstructured document classification.
Box 2: Since PA 12345678 follows a structured pattern, the most effective method is Regular Expression (Regex). A Regular Expression (Regex) can be written to match "PA" followed by exactly eight digits (e.g., PA\s\d{8}). Keyword dictionary is not ideal because it works for predefined words, not number patterns. Function is unnecessary because there is no need for checksum validation or predefined validation rules.

**NEW QUESTION 9**
- (Topic 2)
You have a Microsoft 365 E5 subscription that contains a Microsoft Teams channel named Channel1. Channel1 contains research and development documents.
You plan to implement Microsoft 365 Copilot for the subscription.
You need to prevent the contents of files stored in Channel1 from being included in answers generated by Copilot and shown to unauthorized users.
What should you use?

A. data loss prevention (DLP)
B. Microsoft Purview insider risk management
C. Microsoft Purview Information Barriers
D. sensitivity labels

**Answer:** D

**Explanation:**
To prevent the contents of files stored in Channel1 from being included in Microsoft 365 Copilot responses and ensure unauthorized users cannot access them, you should use Microsoft Purview Sensitivity Labels.
Sensitivity labels allow you to classify, protect, and restrict access to sensitive files. You can configure label-based encryption and access control policies to ensure that only authorized users can access or interact with the files in Channel1. Microsoft 365 Copilot respects sensitivity labels, meaning if a file is labeled with restricted permissions, Copilot will not use it in generated responses for unauthorized users.

**NEW QUESTION 10**
HOTSPOT - (Topic 2)
You have a Microsoft SharePoint Online site that contains the following files.

| Name | Modified by | Data loss prevention (DLP) action |
|---|---|---|
| File1.docx | Manager1 | *None* |
| File2.docx | Manager1 | Matched by DLP |
| File3.docx | Manager1 | Blocked by DLP |

Users are assigned roles for the site as shown in the following table.

| Name | Role |
|---|---|
| User1 | Site owner |
| User2 | Site member |

Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Answer Area**

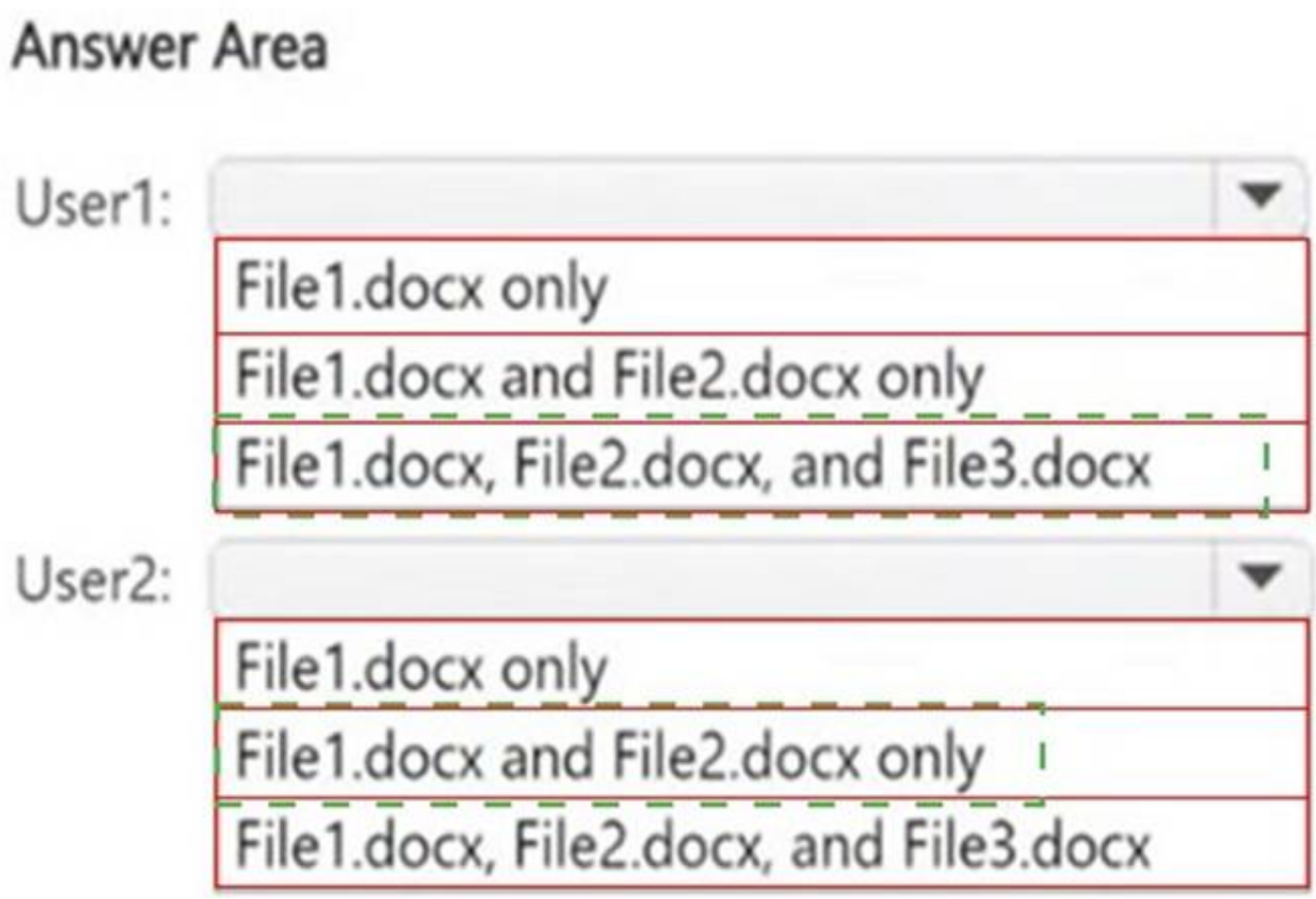
User1:
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

User2:
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

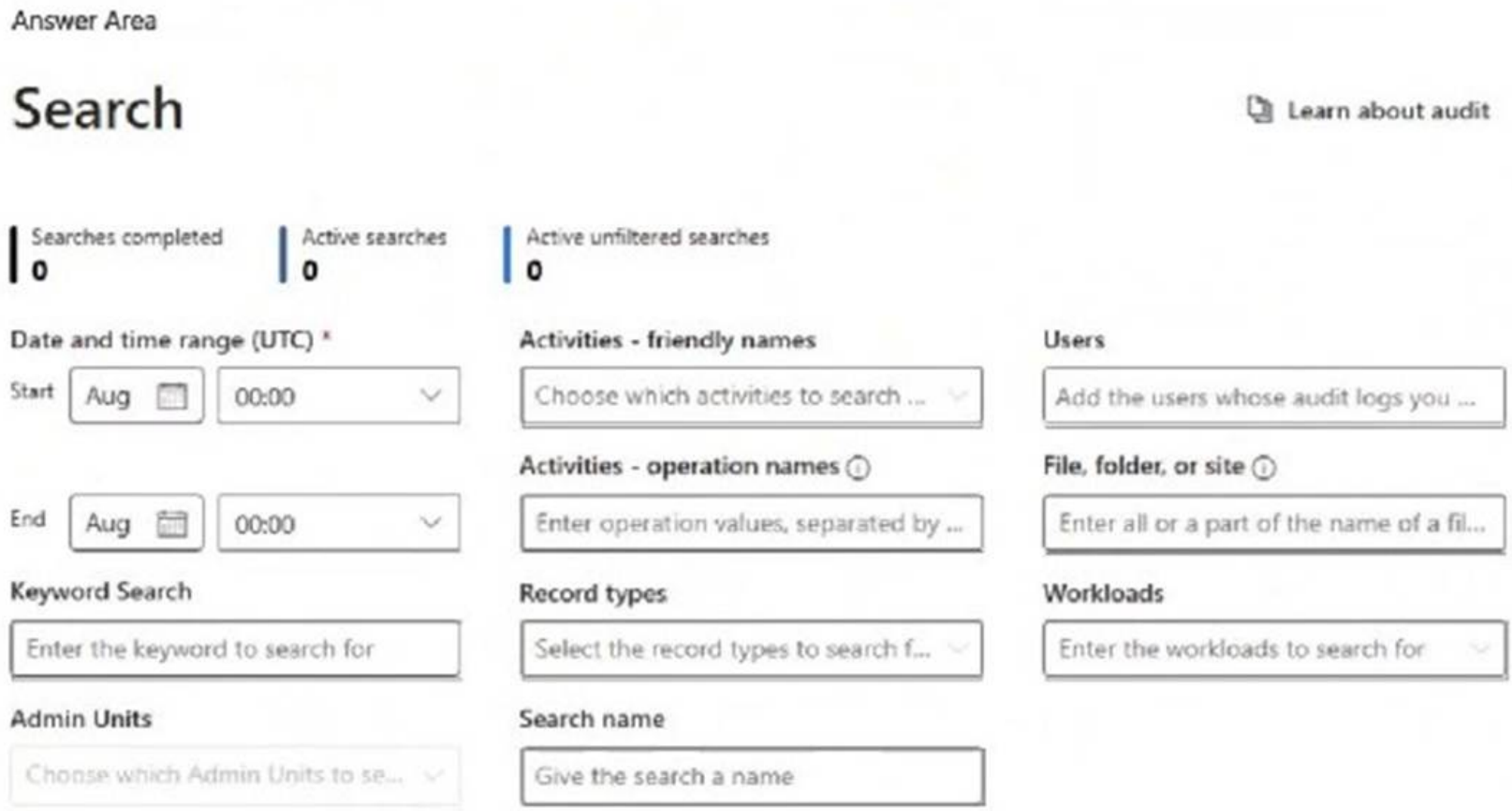
A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**




**NEW QUESTION 10**
HOTSPOT - (Topic 2)
You have a Microsoft 365 subscription.
You plan to deploy an audit log retention policy.
You need to perform a search to validate whether the policy will be applied to the intended entries.
Which two fields should you configure for the search? To answer, select the appropriate fields in the answer area.
NOTE: Each correct selection is worth one point.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
To validate whether an audit log retention policy will apply to the intended entries, you should configure the following fields:
Date and time range (UTC) ensures that you are searching for audit logs within the time period when the policy should be applied. Audit logs are time-sensitive, and policies affect logs based on their timestamp.
Record types allows you to filter and search for specific audit log categories (e.g., Exchange, SharePoint, Teams, etc.) that are affected by the retention policy. Selecting the correct record type ensures that the policy is evaluated against the relevant data.

**NEW QUESTION 13**
- (Topic 2)
You have a Microsoft SharePoint Online site named Site1 that contains a document library. The library contains more than 1,000 documents. Some of the documents are job applicant resumes. All the documents are in the English language.
You plan to apply a sensitivity label automatically to any document identified as a resume. Only documents that contain work experience, education, and accomplishments must be labeled automatically.
You need to identify and categorize the resumes. The solution must minimize administrative effort.
What should you include in the solution?

A. a trainable classifier
B. a keyword dictionary
C. a function
D. an exact data match (EDM) classifier

**Answer:** A

**Explanation:**
Since you need to automatically apply a sensitivity label to resumes based on their content and structure (work experience, education, accomplishments), a trainable classifier is the best choice.
Trainable classifiers use machine learning to identify unstructured data, such as resumes, contracts, or legal documents. Instead of relying on predefined patterns (like keywords or regular expressions), a trainable classifier learns from sample documents and can accurately identify resumes even if they are formatted differently.
Final Approach:
Train a trainable classifier using sample resumes. Deploy the classifier in Microsoft Purview.
Configure a sensitivity label to be automatically applied when a document matches the classifier.

**NEW QUESTION 17**
- (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 21**
- (Topic 2)
You have a Microsoft 365 E5 subscription.
You need to enable support for sensitivity labels in Microsoft SharePoint Online. What should you use?

A. the Microsoft Purview portal
B. the Microsoft Entra admin center
C. the SharePoint admin center
D. the Microsoft 365 admin center

**Answer:** C

**Explanation:**
To enable support for sensitivity labels in Microsoft SharePoint Online, you must configure the setting in the SharePoint admin center.
Sensitivity labels in SharePoint Online allow labeling and protection of files stored in SharePoint and OneDrive. This feature must be enabled in the SharePoint admin center Settings Information protection to allow sensitivity labels to apply encryption and protection to stored documents.

**NEW QUESTION 25**
- (Topic 2)
You have Microsoft 365 E5 subscription that uses data loss prevention (DLP) to protect sensitive information.
You have a document named Form.docx.
You plan to use PowerShell to create a document fingerprint based on Form.docx. You need to first connect to the subscription.
Which cmdlet should you run?

A. Connect-IPPSSession
B. Connect-SPOService
C. Connect-ExchangeOnline
D. Connect-MgGraph

**Answer:** A

**Explanation:**
To create a document fingerprint in Microsoft 365 Data Loss Prevention (DLP), you need to use PowerShell for Microsoft Purview. The correct cmdlet to connect to the Microsoft 365 Security & Compliance Center (where DLP policies are managed) is Connect- IPPSSession. This cmdlet establishes a PowerShell session to manage DLP policies, compliance settings, and document fingerprinting.

**NEW QUESTION 30**
- (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 35**
HOTSPOT - (Topic 2)
You have a Microsoft 365 E5 tenant that contains a sensitivity label named label1. You plan to enable co-authoring for encrypted files.
You need to ensure that files that have label1 applied support co-authoring.
Which two settings should you modify? To answer, select the settings in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

## Access control

Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. Learn more about access control settings

- ○ Remove access control settings if already applied to items
- ◉ Configure access control settings

ⓘ Turn on co-authoring for Office desktop apps so multiple users can simultaneously edit labeled documents that have access control settings applied. Learn more about this setting

Go to co-authoring setting

Assign permissions now or let users decide?

Assign permissions now

The settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires ⓘ

A number of days after label is applied

**Access expires this many days after the label is applied**

90

Allow offline access ⓘ

Always

**Assign permissions to specific users and groups** * ⓘ

Assign permissions

0 items

| Users and groups | Permissions | Edit | Delete |
|---|---|---|---|
| No data available | | | |

☑ Use dynamic watermarking ⓘ

Customize text (optional)

☑ Use Double Key Encryption ⓘ

https://sts.contoso.com

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
C:\Users\Waqas Shahid\Desktop\Mudassir\Untitled.jpg

**NEW QUESTION 39**
HOTSPOT - (Topic 2)
You have a Microsoft 365 E5 subscription.
You receive the data loss prevention (DLP) alert shown in the following exhibit.

Contoso Electronics Microsoft Purview

Sensitive info in email with subject 'Message1'

Details Sensitive info types Metadata

**Event details**

ID
173fe9ac-3a65-41b0-9914-1db451bba639

Location
Exchange

Time of activity
Jun 6, 2022 8:22 PM

**Impacted entities**

User
Megan Bowen

Email recipients
victoria@fabrikam.com

Email subject
Message1

**Policy details**

DLP policy matched
Policy1

Rule matched
Rule1

Sensitive info types detected
Credit Card Number (19, 85%)

Actions taken
GenerateAlert

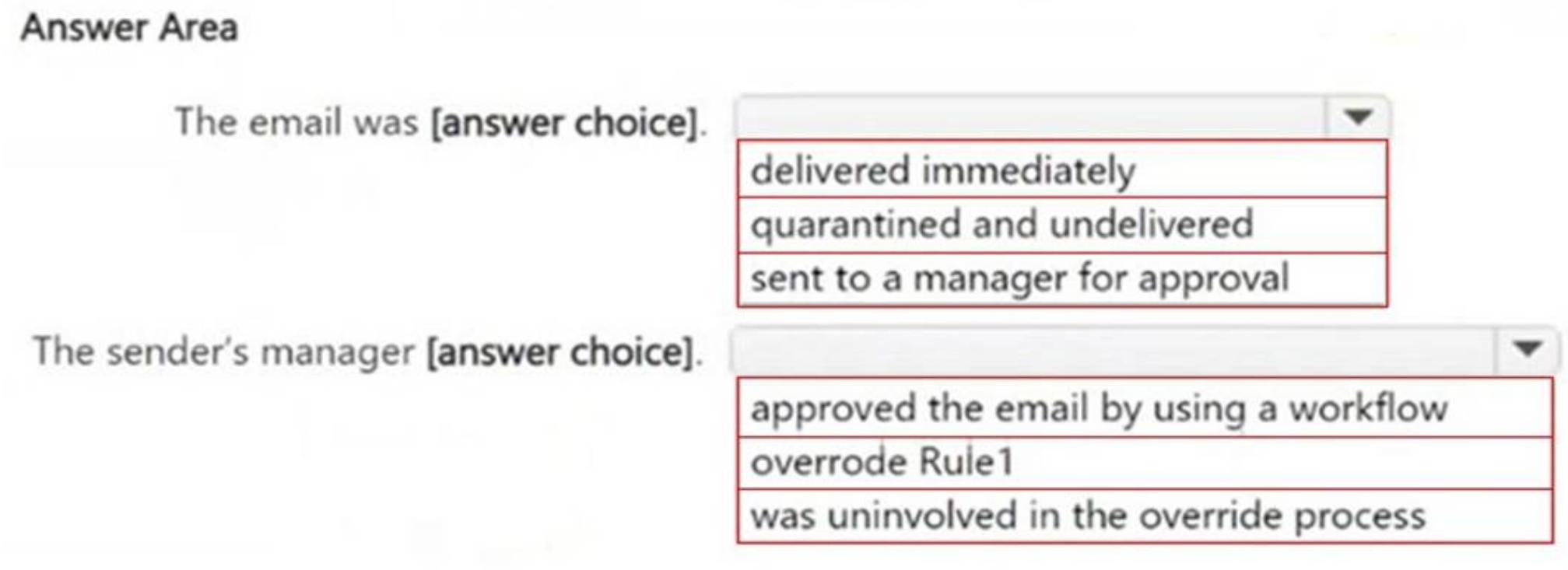
User overrode policy
Yes

Override justification text
Manager approved

Sensitive info detected in
Document1.docx

Actions

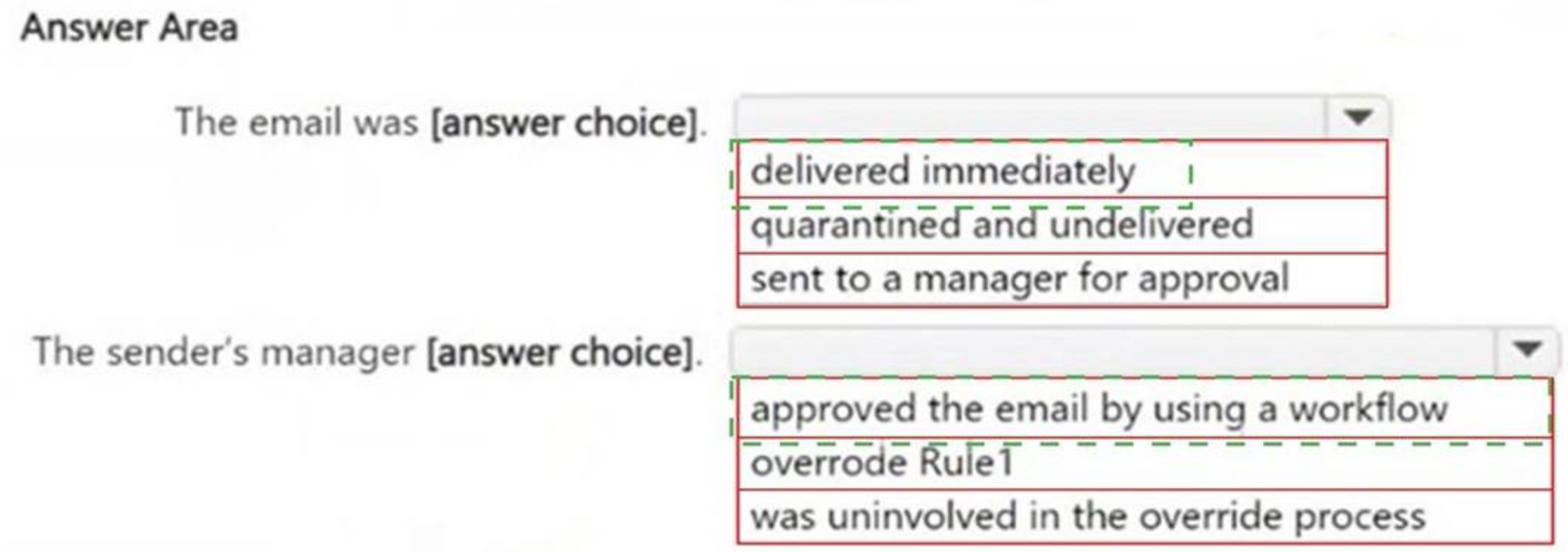
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**




**NEW QUESTION 43**
- (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 grou
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 46**
.....

# Thank You for Trying Our Product

## We offer two products:

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

2nd - Questons 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