Free Microsoft SC-401 Practice Questions

Shared by Blake on 13-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: Hotspot

Case Study: Mix Questions

Mix Questions

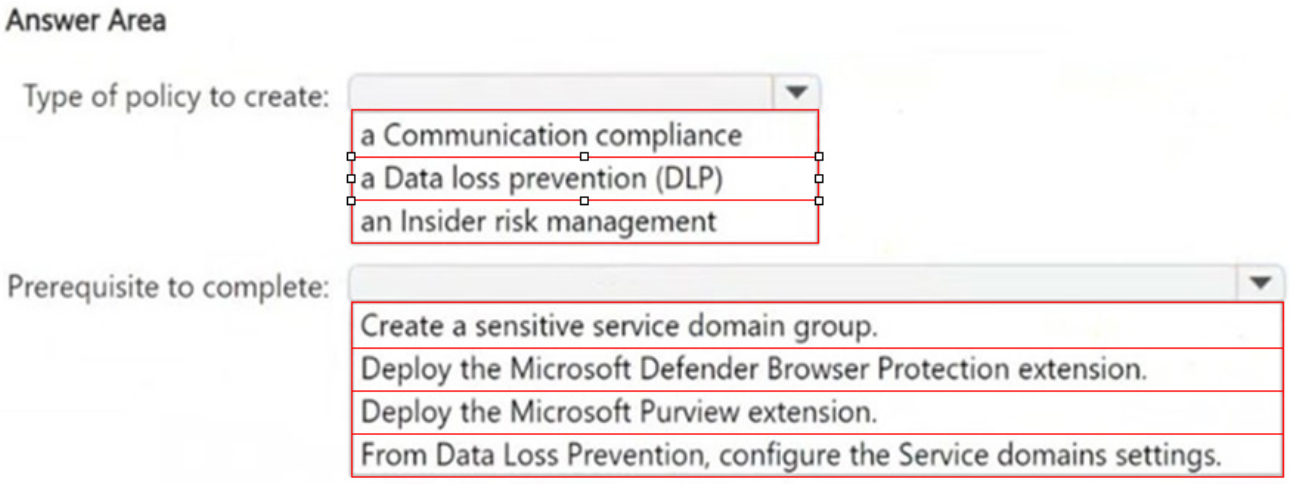
SC-401 Mix Questions IN THIS CASE STUDY

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:

See the Answer in the Premium Version!

Question 2

Question Type: MultipleChoice

You have a Microsoft 365 subscription that contains two Microsoft SharePoint Online sites named Site1 and Site2. You plan to use policies to meet the following requirements:

* Add a watermark of Confidential to a document if the document contains the words Project1 or Project2.

* Retain a document for seven years if the document contains credit card information.

* Add a watermark of Internal Use Only to all the documents stored on Site2.

* Add a watermark of Confidential to all the documents stored on Site1.

You need to recommend the minimum number of sensitive info types required.

How many sensitive info types should you recommend?

Options:

A- 1
B- 2
C- 3
D- 4

Answer:

C

Question 3

Question Type: MultipleChoice

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?

Options:

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

Question 4

Question Type: MultipleChoice

You have a Microsoft J65 subscription linked to a Microsoft Entra tenant that contains a user named User1. You need to grant User1 permission to search Microsoft 365 audit logs. The solution must use the principle of least privilege. Which role should you assign to User1?

Options:

A- the Security Reader role in the Microsoft Entra admin center
B- the Compliance Management role in the Exchange admin center
C- the View Only Audit Logs role in the Exchange admin center
D- the Reviewer role in the Microsoft Purview portal

Answer:

C

Question 5

Question Type: MultipleChoice

You have a Microsoft 365 E5 subscription.

You plan to use insider risk management to collect and investigate forensic evidence.

You need to enable forensic evidence capturing.

What should you do first?

Options:

A- Configure the information protection scanner.
B- Claim capacity.
C- Enable Adaptive Protection.
D- Create priority user groups.

Answer:

B

Question 6

Question Type: MultipleChoice

You implement Microsoft 36S Endpoint data loss pi event ion (Endpoint DIP).

You have computers that run Windows 11 and have Microsoft 365 Apps instated The computers are joined to a Microsoft Entra tenant.

You need to ensure that Endpoint DIP policies can protect content on the computers.

Solution: You onboard the computers to Microsoft Defender for Endpoint Does this meet the goal?

Options:

A- Yes
B- No

Answer:

A

Question 7

Question Type: MultipleChoice

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?

Options:

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.

Question 8

Question Type: MultipleChoice

You have a Microsoft OneDrive folder that contains the files shown in the following table.

Type	Number of files
.jpg	50
.docx	300
.txt	50
.zip	20

In Microsoft Defender for Cloud Apps, you create a file policy to automatically apply a classification. What is the effect of applying the policy?

Options:

A- The policy will apply to only the .docx and .txt files. The policy will classify the files within 24 hours.
B- The policy will apply to only the docx and txt files. The policy will classify the files immediately.
C- The policy will apply to all the files. The policy will classify only 100 files daily.
D- The policy will apply to only the .docx files. The policy will classify only 100 files daily.

Answer:

A

Question 9

Question Type: MultipleChoice

You have a Microsoft 365 E5 subscription.

You need to review a Microsoft 365 Copilot usage report.

From where should you review the report?

Options:

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

Question 10

Question Type: MultipleChoice

You have a Microsoft S65 E5 subscription that contains two users named User! and Admin1 Admin1 manages audit retention policies for the subscription.

You need to ensure that the audit logs of User1 will be retained for 10 years.

What should you do first?

Options:

A- Assign a Microsoft Purview Audit (Premium) add on license to User1.
B- Assign a 10 year audit log retention add-on license to Admin1.
C- Assign a 10-year audit log retention add-on license to User1.
D- Assign a Microsoft Purview Audit (Premium) add-on license to Admin1.

Answer:

C

Question 11

Question Type: MultipleChoice

You have a Microsoft 365 E5 subscription.

You need to ensure that encrypted email messages sent to an external recipient can be revoked or will expire within seven days.

What should you configure first?

Options:

A- a custom branding template
B- a mail flow rule
C- a sensitivity label
D- a Conditional Access policy

Answer:

C

Explanation:

To ensure that encrypted email messages sent to external recipients can be revoked or expire within seven days, you need to configure a sensitivity label with encryption settings in Microsoft Purview Information Protection. A sensitivity label allows you to encrypt emails and documents, set expiration policies (e.g., emails expire after 7 days), and enable email revocation

How to configure it?

Go to Microsoft Purview compliance portal Information Protection

Create a sensitivity label

Enable encryption and configure the content expiration policy

Publish the label to users