

KillTest

Higher Quality, Better Service!



Q&A

<http://www.killtest.com>

We offer free update service for one year.

Exam : SC-401

**Title : Administering Information
Security in Microsoft 365**

Version : DEMO

1.DRAG DROP

Case Study

Instructions

This is a case study. Case studies are not timed separately from other exam sections. You can use as much exam time as you would like to complete each case study. However, there might be additional case studies or other exam sections. Manage your time to ensure that you can complete all the exam sections in the time provided. Pay attention to the Exam Progress at the top of the screen so you have sufficient time to complete any exam sections that follow this case study.

To answer the case study questions, you will need to reference information that is provided in the case. Case studies and associated questions might contain exhibits or other resources that provide more information about the scenario described in the case. Information provided in an individual question does not apply to the other questions in the case study.

A Review Screen will appear at the end of this case study. From the Review Screen, you can review and change your answers before you move to the next exam section. After you leave this case study, you will NOT be able to return to it.

To start the case study

To display the first question in this case study, select the "Next" button. To the left of the question, a menu provides links to information such as business requirements, the existing environment, and problem statements. Please read through all this information before answering any questions. When you are ready to answer a question, select the "Question" button to return to the question.

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.

Existing Environment

Microsoft 365 Environment

Contoso has a Microsoft 365 E5 tenant.

The tenant contains the administrative user accounts shown in the following table.

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

Users store data in the following locations:

- SharePoint sites

- OneDrive accounts
- Exchange email
- Exchange public folders
- Teams chats
- Teams channel messages

When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

SharePoint Online Environment

Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.

Site2 contains the files shown in the following table.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.

Site4 has the following two retention policies applied:

- Name: Site4RetentionPolicy1
- Locations to apply the policy: Site4
- Delete items older than: 2 years
- Delete content based on: When items were created
- Name: Site4RetentionPolicy2
- Locations to apply the policy: Site4
- Retain items for a specific period: 4 years
- Start the retention period based on: When items were created
- At the end of the retention period: Do nothing

Problem Statements

Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

Requirements

Planned Changes

Contoso plans to create the following data loss prevention (DLP) policy:

- Name: DLPpolicy1
- Locations to apply the policy: Site2
- Conditions:
 - Content contains any of these sensitive info types: SWIFT Code
 - Instance count: 2 to any
- Actions: Restrict access to the content

Technical Requirements

Contoso must meet the following technical requirements:

- All administrative users must be able to review DLP reports.
- Whenever possible, the principle of least privilege must be used.
- For all users, all Microsoft 365 data must be retained for at least one year.
- Confidential documents must be detected and protected by using Microsoft 365.
- Site1 documents that include credit card numbers must be labeled automatically.
- All administrative users must be able to create Microsoft 365 sensitivity labels.
- After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.

You need to meet the technical requirements for the Site1 documents.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Create a sensitivity label.	
Wait 24 hours and then turn on the policy.	
Create a sensitive info type.	
Create a retention label.	
Create an auto-labeling policy.	

Answer:

Actions	Answer Area
Create a sensitivity label.	Create a sensitive info type.
Wait 24 hours and then turn on the policy.	Create a sensitivity label.
Create a sensitive info type.	Create an auto-labeling policy.
Create a retention label.	
Create an auto-labeling policy.	

2.Case Study

Instructions

This is a case study. Case studies are not timed separately from other exam sections. You can use as much exam time as you would like to complete each case study. However, there might be additional case studies or other exam sections. Manage your time to ensure that you can complete all the exam sections in the time provided. Pay attention to the Exam Progress at the top of the screen so you have sufficient time to complete any exam sections that follow this case study.

To answer the case study questions, you will need to reference information that is provided in the case. Case studies and associated questions might contain exhibits or other resources that provide more information about the scenario described in the case. Information provided in an individual question does not apply to the other questions in the case study.

A Review Screen will appear at the end of this case study. From the Review Screen, you can review and change your answers before you move to the next exam section. After you leave this case study, you will NOT be able to return to it.

To start the case study

To display the first question in this case study, select the "Next" button. To the left of the question, a menu provides links to information such as business requirements, the existing environment, and problem statements. Please read through all this information before answering any questions. When you are ready to answer a question, select the "Question" button to return to the question.

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.

Existing Environment

Microsoft 365 Environment

Contoso has a Microsoft 365 E5 tenant.

The tenant contains the administrative user accounts shown in the following table.

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

Users store data in the following locations:

- SharePoint sites
- OneDrive accounts
- Exchange email
- Exchange public folders
- Teams chats
- Teams channel messages

When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

SharePoint Online Environment

Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4. Site2 contains the files shown in the following table.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.

Site4 has the following two retention policies applied:

- Name: Site4RetentionPolicy1
- Locations to apply the policy: Site4
- Delete items older than: 2 years
- Delete content based on: When items were created

- Name: Site4RetentionPolicy2
- Locations to apply the policy: Site4
- Retain items for a specific period: 4 years
- Start the retention period based on: When items were created
- At the end of the retention period: Do nothing

Problem Statements

Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

Requirements

Planned Changes

Contoso plans to create the following data loss prevention (DLP) policy:

- Name: DLPpolicy1
- Locations to apply the policy: Site2
- Conditions:
 - Content contains any of these sensitive info types: SWIFT Code
 - Instance count: 2 to any
- Actions: Restrict access to the content

Technical Requirements

Contoso must meet the following technical requirements:

- All administrative users must be able to review DLP reports.
- Whenever possible, the principle of least privilege must be used.
- For all users, all Microsoft 365 data must be retained for at least one year.
- Confidential documents must be detected and protected by using Microsoft 365.
- Site1 documents that include credit card numbers must be labeled automatically.
- All administrative users must be able to create Microsoft 365 sensitivity labels.
- After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.

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: B

3.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 (IBs)
- D. sensitivity labels

Answer: D

4.DRAG DROP

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	Answer Area	Filter
Access level	When a file is shared externally.	
Collaborators	When a file is labelled as Internal only.	
Matched policy		
Sensitivity label		

Answer:

Filters	Answer Area	Filter
Access level	When a file is shared externally.	Access level
Collaborators	When a file is labelled as Internal only.	Sensitivity label
Matched policy		
Sensitivity label		

5.HOTSPOT

You have a Microsoft 365 E5 subscription that contains three DOCX files named File1, File2, and File3.

You create the sensitivity labels shown in the following table.

Name	Permission	Apply content marking
Label1	Any authenticated users: Viewer	Disabled
Label2	None	Enabled

You apply the labels to the files as shown in the following table.

File	Label
File1	<i>None</i>
File2	Label1
File3	Label2

You ask Microsoft 365 Copilot to summarize the files, and you receive the results shown in the following table.

Name	Based on content of
Summary1	File1, File3
Summary2	File2
Summary3	File1, File2, File3

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
Summary1 has a sensitivity label applied.	☐	☐
Summary2 has a sensitivity label applied.	☐	☐
Summary3 has a sensitivity label applied.	☐	☐

Answer:

Answer Area

Statements	Yes	No
Summary1 has a sensitivity label applied.	☒	☐
Summary2 has a sensitivity label applied.	☒	☐
Summary3 has a sensitivity label applied.	☒	☐