

Microsoft.SC-400.vAug-2024.by.Lion.155q

Number: SC-400
Passing Score: 800
Time Limit: 120
File Version: 12.0

Exam Code: SC-400
Exam Name: Microsoft Information Protection Administrator



01 - Implement Data Loss Prevention

QUESTION 1

Your company has a Microsoft 365 tenant that uses a domain named contoso.com.

You are implementing data loss prevention (DLP).

The company's default browser is Microsoft Edge.

During a recent audit, you discover that some users use Firefox and Google Chrome browsers to upload files labeled as Confidential to a third-party Microsoft SharePoint Online site that has a URL of <https://m365x076709.sharepoint.com>.

Users are blocked from uploading the confidential files to the site from Microsoft Edge.

You need to ensure that the users cannot upload files labeled as Confidential from Firefox and Google Chrome to any cloud services. Which two actions should you perform? Each correct answer presents part of the solution. (Choose two.)

NOTE: Each correct selection is worth one point.

- A. From the Microsoft 365 Endpoint data loss prevention (Endpoint) DLP settings, add m365x076709.sharepoint.com as a blocked service domain.
- B. Create a DLP policy that applies to the Devices location.
- C. From the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings, add Firefox and Google Chrome to the unallowed browsers list.
- D. From the Microsoft 365 compliance center, onboard the devices.
- E. From the Microsoft 365 Endpoint data loss prevention (Endpoint) DLP settings, add contoso.com as an allowed service domain.

Correct Answer: C, D

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about?view=o365-worldwide>



QUESTION 2

HOTSPOT

You have a Microsoft SharePoint Online site that contains the following files.

Name	Modified by	Data loss prevention (DLP) status
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 view? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

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

Answer Area:

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



Section:

Explanation:

Reference:

<https://social.technet.microsoft.com/wiki/contents/articles/36527.implement-data-loss-prevention-dlp-in-sharepoint-online.aspx>

QUESTION 3

HOTSPOT

You have a Microsoft 365 tenant that uses Microsoft Teams.

You create a data loss prevention (DLP) policy to prevent Microsoft Teams users from sharing sensitive information.

You need to identify which locations must be selected to meet the following requirements:

Documents that contain sensitive information must not be shared inappropriately in Microsoft Teams. If a user attempts to share sensitive information during a Microsoft Teams chat session, the message must be deleted immediately. Which three locations should you select? To answer, select the appropriate locations in the answer area. (Choose three.)
NOTE: Each correct selection is worth one point.


Hot Area:

Answer Area

Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

Status	Location	Included
<input type="checkbox"/> Off	Exchange email	<input type="checkbox"/>
<input type="checkbox"/> Off	SharePoint sites	<input type="checkbox"/>
<input type="checkbox"/> Off	OneDrive accounts	<input type="checkbox"/>
<input type="checkbox"/> Off	Teams chat and channel messages	<input type="checkbox"/>
<input type="checkbox"/> Off	Microsoft Cloud App Security	<input type="checkbox"/>



Answer Area:

Answer Area

Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

Status	Location	Included
<input type="checkbox"/> Off	Exchange email	
<input checked="" type="checkbox"/> Off	SharePoint sites	
<input checked="" type="checkbox"/> Off	OneDrive accounts	
<input checked="" type="checkbox"/> Off	Teams chat and channel messages	
<input type="checkbox"/> Off	Microsoft Cloud App Security	

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-microsoft-teams?view=o365-worldwide>

QUESTION 4

HOTSPOT

You have a data loss prevention (DLP) policy that has the advanced DLP rules shown in the following table.

Name	Priority	Actions
Rule1	0	<ul style="list-style-type: none">• Notify users with email and policy tips• User overrides: Off
Rule2	1	<ul style="list-style-type: none">• Notify users with email and policy tips• Restrict access to the content• User overrides: Off
Rule3	2	<ul style="list-style-type: none">• Notify users with email and policy tips• Restrict access to the content• User overrides: On
Rule4	3	<ul style="list-style-type: none">• Notify users with email and policy tips• Restrict access to the content• User overrides: Off

You need to identify which rules will apply when content matches multiple advanced DLP rules. Which rules should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

If content matches Rule1, Rule2, and Rule3:

- Only Rule1 takes effect
- Only Rule2 takes effect
- Only Rule3 takes effect
- Rule1, Rule2, and Rule3 take effect

If content matches Rule2, Rule3, and Rule4:

- Only Rule2 takes effect
- Only Rule3 takes effect
- Only Rule4 takes effect
- Only Rule2 and Rule4 take effect
- Rule2, Rule3, and Rule4 take effect

Answer Area:

Answer Area

If content matches Rule1, Rule2, and Rule3:

▼
Only Rule1 takes effect
Only Rule2 takes effect
Only Rule3 takes effect
Rule1, Rule2, and Rule3 take effect

If content matches Rule2, Rule3, and Rule4:

▼
Only Rule2 takes effect
Only Rule3 takes effect
Only Rule4 takes effect
Only Rule2 and Rule4 take effect
Rule2, Rule3, and Rule4 take effect

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide>

QUESTION 5

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

- A. From the Microsoft 365 compliance center, create a data loss prevention (DLP) policy.
- B. From the Microsoft 365 compliance center, start a data investigation.
- C. From the Microsoft 365 compliance center, create an insider risk policy.
- D. From the Cloud App Security portal, create an activity policy.

Correct Answer: A

Section:

Explanation:

With a DLP policy, you can identify, monitor, and automatically protect sensitive items.

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

1. From the Microsoft 365 compliance center, create a data loss prevention (DLP) policy.
2. From the Cloud App Security portal, create a file policy.

Other incorrect answer options you may see on the exam include the following:

From the Exchange admin center, create a data loss prevention (DLP) policy.

From the Microsoft 365 compliance center, create an insider risk policy. From the Azure portal, create an Azure Information Protection policy.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide>

QUESTION 6

You need to protect documents that contain credit card numbers from being opened by users outside your company. The solution must ensure that users at your company can open the documents. What should you use?

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

Correct Answer: D

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide>

QUESTION 7

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

You have the users shown in the following table.

Name	Group/role
User1	Site1 member group
User2	Site1 member group
User3	Site1 owner group
User4	Sharepoint administrator role

You create a data loss prevention (DLP) policy for Site1 that detects credit card number information. You configure the policy to use the following protection action:

When content matches the policy conditions, show policy tips to users and send them an email notification.

You use the default notification settings.

To Site1, User1 uploads a file that contains a credit card number.

Which users receive an email notification?

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

Correct Answer: D

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-the-default-dlp-policy?view=o365-worldwide>

QUESTION 8

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 implement Microsoft 365 Endpoint data loss prevention (Endpoint DLP).

You have computers that run Windows 10 and have Microsoft 365 Apps installed. The computers are joined to Azure Active Directory (Azure AD).

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

Solution: You deploy the Endpoint DLP configuration package to the computers.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started?view=o365-worldwide> <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints?view=o365-worldwide>

QUESTION 9

You create a data loss prevention (DLP) policy. The Advanced DLP rules page is shown in the Rules exhibit.

Data loss prevention > **Create policy**

Name	Status	Edit	Move
^ DLP rule 1	<input checked="" type="checkbox"/> On		

Conditions
Content contains any of these sensitive info types:
- Argentina National Identity (DNI) Number
Content is shared from Microsoft 365 with people outside my organization

Actions
- Notify users with email and policy tips
- Restrict access to the content
- Send incident reports to Administrator
- Send alerts to Administrator

The Review your settings page is shown in the Review exhibit.

Review your policy and create it
Review all settings for your new DLP policy and create it.

The information to protect
Custom policy

Name
Contractor ID Numbers

Description
Create a custom policy from scratch. You will choose the type of content to protect and how you want to protect it.

Locations to apply the policy
Exchange email
SharePoint sites
OneDrive accounts
Teams chat and channel messages
Devices
Microsoft Cloud App Security

Policy settings
DLP rule 1

Turn policy on after it's created?
No



You need to review the potential impact of enabling the policy without applying the actions. What should you do?

- A. Edit the policy, remove all the actions in DLP rule 1, and select I'd like to test it out first.
- B. Edit the policy, remove the Restrict access to the content and Send incident report to Administrator actions, and then select Yes, turn it on right away.
- C. Edit the policy, remove all the actions in DLP rule 1, and select Yes, turn it on right away.
- D. Edit the policy, and then select I'd like to test it out first.

Correct Answer: D

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-dlp-policy-from-a-template?view=o365-worldwide>

QUESTION 10

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 keys in plain text to third parties.

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

Solution: You configure a mail flow rule that matches a sensitive info type.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Section:

QUESTION 11

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 keys in plain text to third parties.

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

Solution: You create a data loss prevention (DLP) policy that has all locations selected.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

QUESTION 12

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 keys in plain text to third parties.

You need to ensure that when Azure Storage 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

Correct Answer: B

Section:

QUESTION 13

You are creating an advanced data loss prevention (DLP) rule in a DLP policy named Policy 1 that will have all locations selected.

Which two conditions can you use in the rule? Each correct answer presents a complete solution. (Choose two.)

NOTE: Each correct selection is worth one point.



- A. Content contains
- B. Content is shared from Microsoft 365
- C. Document size equals or is greater than
- D. Attachment's file extension is
- E. Document property is

Correct Answer: A, B

Section:

QUESTION 14

You need to provide a user with the ability to view data loss prevention (DLP) alerts in the Microsoft 365 compliance center. The solution must use the principle of least privilege. Which role should you assign to the user?

- A. Compliance data administrator
- B. Security operator
- C. Compliance administrator
- D. Security reader

Correct Answer: D

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-worldwide>

QUESTION 15

HOTSPOT

You create a data loss prevention (DLP) policy that meets the following requirements:

Prevents guest users from accessing a sensitive document shared during a Microsoft Teams chat

Prevents guest users from accessing a sensitive document stored in a Microsoft Teams channel

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Prevents guest users from accessing a sensitive document shared during a Microsoft Teams chat:

- Exchange email
- OneDrive accounts
- SharePoint sites
- Teams chat and channel messages

Prevents guest users from accessing a sensitive document stored in a Microsoft Teams channel:

- Exchange email
- OneDrive accounts
- SharePoint sites
- Teams chat and channel messages



Answer Area:

Answer Area

Prevents guest users from accessing a sensitive document shared during a Microsoft Teams chat:

Exchange email
OneDrive accounts
SharePoint sites
Teams chat and channel messages

Prevents guest users from accessing a sensitive document stored in a Microsoft Teams channel:

Exchange email
OneDrive accounts
SharePoint sites
Teams chat and channel messages

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-microsoft-teams?view=o365-worldwide>

<https://docs.microsoft.com/en-us/microsoftteams/sharepoint-onedrive-interact>

QUESTION 16

HOTSPOT

You have a Microsoft 365 E5 tenant.

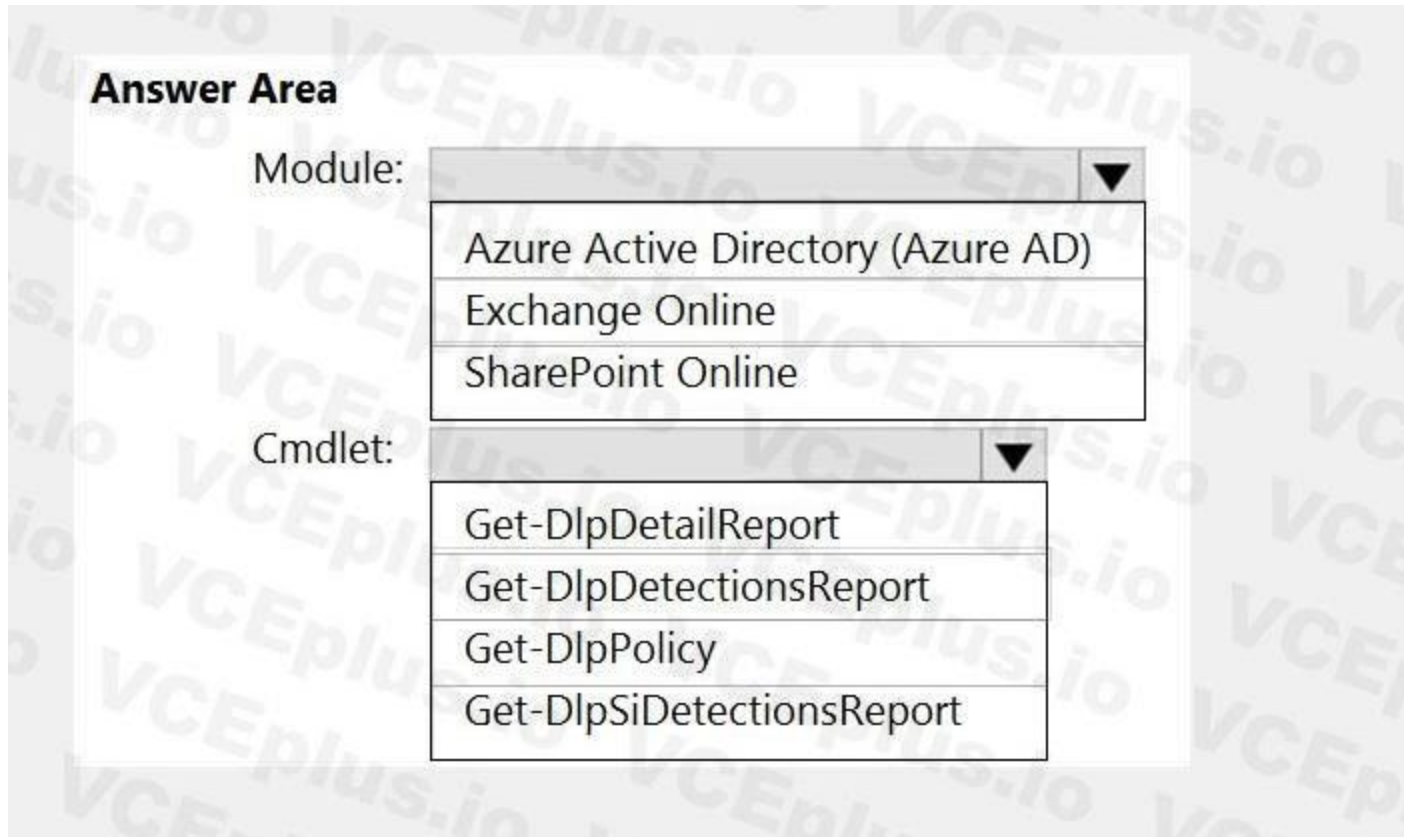
Data loss prevention (DLP) policies are applied to Exchange email, SharePoint sites, and OneDrive accounts locations.

You need to use PowerShell to retrieve a summary of the DLP rule matches from the last seven days.

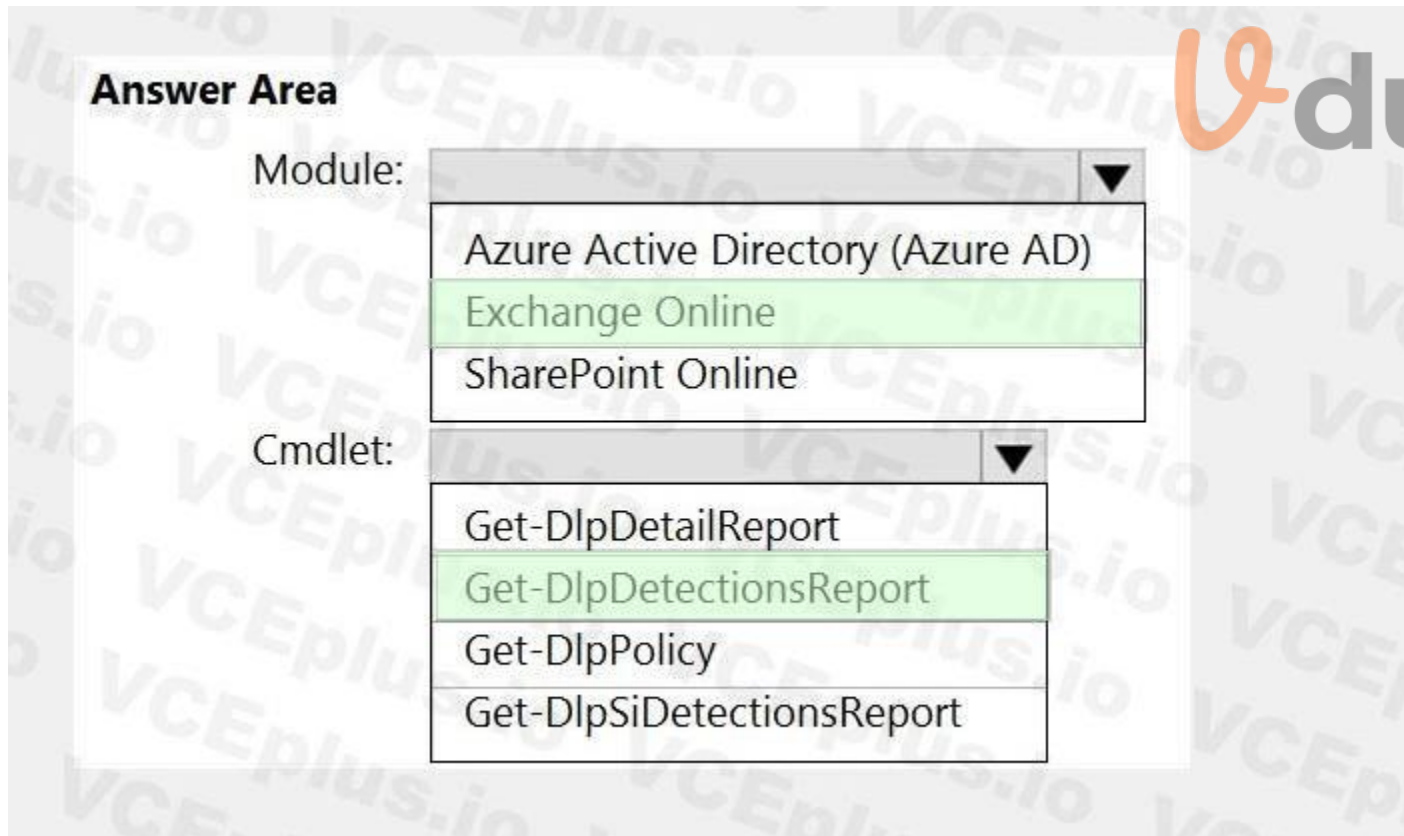
Which PowerShell module and cmdlet should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/powershell/module/exchange/get-dlpdetectionsreport?view=exchange-ps>

QUESTION 17

HOTSPOT

You plan to implement Microsoft 365 Endpoint data loss prevention (Endpoint DLP).

You need to identify which end user activities can be audited on the endpoints, and which activities can be restricted on the endpoints.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Print a protected document:

<input type="checkbox"/>	Can be audited only
<input type="checkbox"/>	Can be restricted only
<input type="checkbox"/>	Can be audited and restricted

Create a document in a monitored location:

<input type="checkbox"/>	Can be audited only
<input type="checkbox"/>	Can be restricted only
<input type="checkbox"/>	Can be audited and restricted

Copy a protected document to USB removable media:

<input type="checkbox"/>	Can be audited only
<input type="checkbox"/>	Can be restricted only
<input type="checkbox"/>	Can be audited and restricted

Answer Area:

Answer Area

Print a protected document:

Can be audited only
Can be restricted only
Can be audited and restricted

Create a document in a monitored location:

Can be audited only
Can be restricted only
Can be audited and restricted

Copy a protected document to USB removable media:

Can be audited only
Can be restricted only
Can be audited and restricted

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about?view=o365-worldwide>

QUESTION 18

You have a data loss prevention (DLP) policy that applies to the Devices location. The policy protects documents that contain United States passport numbers.

Users report that they cannot upload documents to a travel management website because of the policy.

You need to ensure that the users can upload the documents to the travel management website. The solution must prevent the protected content from being uploaded to other locations.

Which Microsoft 365 Endpoint data loss prevention (Endpoint DLP) setting should you configure?

- A. Unallowed browsers
- B. File path exclusions
- C. Unallowed apps
- D. Service domains

Correct Answer: D

Section:

Explanation:

You can control whether sensitive files protected by your policies can be uploaded to specific service domains from Microsoft Edge.

If the list mode is set to Block, then user will not be able to upload sensitive items to those domains. When an upload action is blocked because an item matches a DLP policy, DLP will either generate a warning or block the upload of the sensitive item.

If the list mode is set to Allow, then users will be able to upload sensitive items only to those domains, and upload access to all other domains is not allowed.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide>

QUESTION 19

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

Name	Type
Device1	Windows 8.1
Device2	Windows 10
Device3	iOS
Device4	macOS
Device5	CentOS Linux

You plan to start using Microsoft 365 Endpoint data loss protection (Endpoint DLP).

Which devices support Endpoint DLP?

- A. Device5 only
- B. Device2 only
- C. Device1, Device2, Device3, Device4, and Device5
- D. Device3 and Device4 only
- E. Device1 and Device2 only



Correct Answer: B

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about?view=o365-worldwide>

QUESTION 20

A compliance administrator recently created several data loss prevention (DLP) policies.

After the policies are created, you receive a higher than expected volume of DLP alerts.

You need to identify which rules are generating the alerts.

Which DLP report should you use?

- A. Third-party DLP policy matches
- B. DLP policy matches
- C. DLP incidents
- D. False positive and override

Correct Answer: B

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide>

QUESTION 21

HOTSPOT

You have a Microsoft 365 tenant that uses data loss prevention (DLP) to protect sensitive information. You create a new custom sensitive info type that has the matching element shown in the following exhibit.

Matching element

^ Detect content containing

Regular expression v

`^\d{3}(-){3}\d{3}\d{12}$`

The supporting elements are configured as shown in the following exhibit.

Supporting elements

^ Contains this keyword list

Keyword list

Minimum Count

"Employee ID"

1

The confidence level and character proximity are configured as shown in the following exhibit.

Confidence level i

Default (60%) 75

Character proximity i

Default (300 characters) 100

For each of the following statements, select Yes if statement is true. Otherwise, select No
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements

A document that contains the following text will match the sensitive info type: James has an Employee ID of 555-343-111-065. Yes No

A document that contains the following text will match the sensitive info type: The Employee ID of the employee Ben Smith is 555343123444. Yes No

A document that contains the following text will match the sensitive info type: The id badge for 555-123 has expired. Yes No

Answer Area:


Answer Area

Statements

A document that contains the following text will match the sensitive info type: James has an Employee ID of 555-343-111-065. Yes No

A document that contains the following text will match the sensitive info type: The Employee ID of the employee Ben Smith is 555343123444. Yes No

A document that contains the following text will match the sensitive info type: The id badge for 555-123 has expired. Yes No



Section:

Explanation:

Note: The regular expression has a starts with (^) and ends with (\$) metacharacter and will not match any of the sentences. Without the starts with (^) metacharacter the first and second sentences would match and the supporting element (Employee ID) would be within 100 character proximity.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-custom-sensitive-information-type?view=o365-worldwide>

QUESTION 22

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 10. The computers are onboarded to the Microsoft 365 compliance center.

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 the Cloud App Security portal, you create an app discovery policy.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

Explanation:

You can create app discovery policies to alert you when new apps are detected within your organization.

Use the unallowed apps list instead.

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/cloud-discovery-policies>

<https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide>

QUESTION 23

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 10. The computers are onboarded to the Microsoft 365 compliance center.

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 the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings, you add a folder path to the file path exclusions.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

Explanation:

Folder path to the file path exclusions excludes certain paths and files from DLP monitoring.

Use the unallowed apps list instead.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide>

QUESTION 24

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 10. The computers are onboarded to the Microsoft 365 compliance center.

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 the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings, you add the application to the unallowed apps list.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section:

Explanation:

Unallowed apps is a list of applications that you create which will not be allowed to access a DLP protected file.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide>

QUESTION 25

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 are configuring a file policy in Microsoft Cloud App Security.

You need to configure the policy to apply to all files. Alerts must be sent to every file owner who is affected by the policy. The policy must scan for credit card numbers, and alerts must be sent to the Microsoft Teams site of the affected department.

Solution: You use the Data Classification service inspection method and send alerts as email.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

Explanation:

Alerts must be sent to the Microsoft Teams site of the affected department. A Microsoft Power Automate playbook should be used.

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/dcs-inspection>

<https://docs.microsoft.com/en-us/cloud-app-security/flow-integration>

QUESTION 26

You are planning a data loss prevention (DLP) solution that will apply to computers that run Windows 10.

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

Correct Answer: A

Section:

QUESTION 27

You need to be alerted when users share sensitive documents from Microsoft One Drive to any users outside your company.

What should you do?



- A. From the Exchange admin center, create a data loss prevention (DLP) policy.
- B. From the Azure portal, create an Azure Active Directory (Azure AD) Identity Protection policy.
- C. From the Microsoft 365 compliance center, create an insider risk policy.
- D. From the Cloud App Security portal, create a file policy.

Correct Answer: D

Section:

Explanation:

File Policies allow you to enforce a wide range of automated processes using the cloud provider's APIs. Policies can be set to provide continuous compliance scans, legal eDiscovery tasks, DLP for sensitive content shared publicly, and many more use cases.

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

1. From the Microsoft 365 compliance center, create a data loss prevention (DLP) policy.
2. From the Cloud App Security portal, create a file policy.

Other incorrect answer options you may see on the exam include the following:

From the Microsoft 365 compliance center, start a data investigation.

From the Azure portal, create an Azure Information Protection policy.

Reference:

<https://docs.microsoft.com/en-us/defender-cloud-apps/data-protection-policies>

QUESTION 28

Your company has a Microsoft 365 tenant.

The company performs annual employee assessments. The assessment results are recorded in a document named AssessmentTemplate.docx that is created by using a Microsoft Word template. Copies of the employee assessments are sent to employees and their managers. The assessment copies are stored in mailboxes, Microsoft SharePoint Online sites, and OneDrive for Business folders. A copy of each assessment is also stored in a SharePoint Online folder named Assessments.

You need to create a data loss prevention (DLP) policy that prevents the employee assessments from being emailed to external users. You will use a document fingerprint to identify the assessment documents. The solution must minimize effort.

What should you include in the solution?

- A. Create a fingerprint of 100 sample documents in the Assessments folder.
- B. Create a sensitive info type that uses Exact Data Match (EDM).
- C. Import 100 sample documents from the Assessments folder to a seed folder.
- D. Create a fingerprint of AssessmentTemplate.docx.

Correct Answer: D

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/document-fingerprinting?view=o365-worldwide>

QUESTION 29

You have a Microsoft 365 subscription that uses Microsoft Exchange Online.

You need to receive an alert if a user emails sensitive documents to specific external domains.

What should you create?

- A. a data loss prevention (DLP) policy that uses the Privacy category

- B. a Microsoft Cloud App Security activity policy
- C. a Microsoft Cloud App Security file policy
- D. a data loss prevention (DLP) alert filter

Correct Answer: A

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-reference?view=o365-worldwide>

QUESTION 30

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 10. The computers are onboarded to the Microsoft 365 compliance center.

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 the Cloud App Security portal, you mark the application as Unsanctioned.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide>



QUESTION 31

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 keys in plain text to third parties.

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

Solution: You configure a mail flow rule that matches the text patterns.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/exchange/policy-and-compliance/mail-flow-rules/conditions-and-exceptions?view=exchserver-2019>

QUESTION 32

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 are configuring a file policy in Microsoft Cloud App Security.

You need to configure the policy to apply to all files. Alerts must be sent to every file owner who is affected by the policy. The policy must scan for credit card numbers, and alerts must be sent to the Microsoft Teams site of the affected department.

Solution: You use the Built-in DLP inspection method and send alerts to Microsoft Power Automate.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/content-inspection-built-in>

<https://docs.microsoft.com/en-us/cloud-app-security/flow-integration>

QUESTION 33

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 are configuring a file policy in Microsoft Cloud App Security.

You need to configure the policy to apply to all files. Alerts must be sent to every file owner who is affected by the policy. The policy must scan for credit card numbers, and alerts must be sent to the Microsoft Teams site of the affected department.

Solution: You use the Built-in DLP inspection method and send alerts as email.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

Explanation:

Alerts must be sent to the Microsoft Teams site of the affected department. A Microsoft Power Automate playbook should be used.

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/content-inspection-built-in>

<https://docs.microsoft.com/en-us/cloud-app-security/flow-integration>

QUESTION 34

You have a Microsoft 365 tenant that uses 100 data loss prevention (DLP) policies.

A Microsoft Exchange administrator frequently investigates emails that were blocked due to DLP policy violations.

You need recommend which DLP report the Exchange administrator can use to identify how many messages were blocked based on each DLP policy.

Which report should you recommend?

- A. Third-party DLP policy matches
- B. DLP policy matches
- C. DLP incidents
- D. False positive and override

Correct Answer: B

Section:

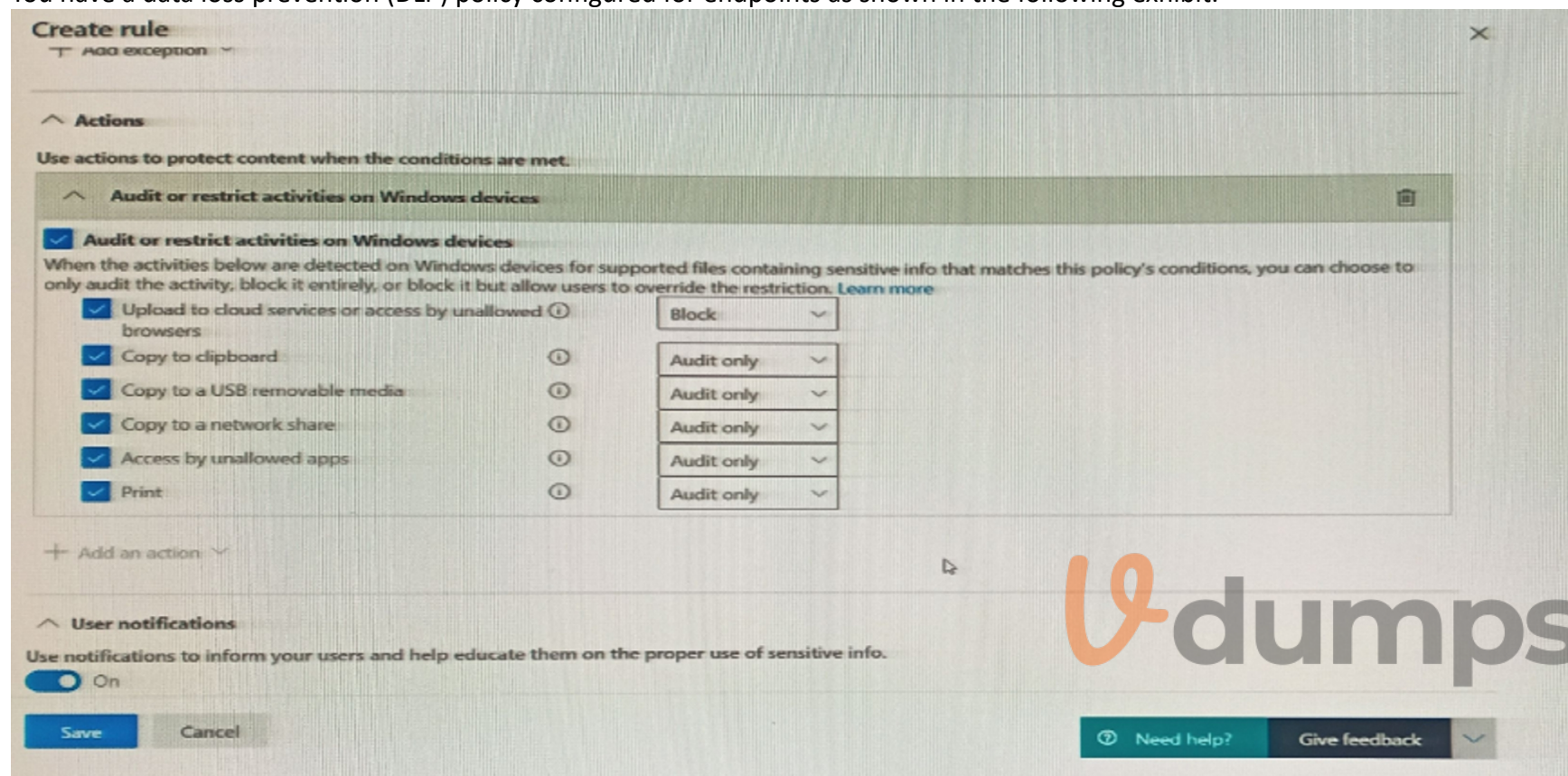
Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide>

QUESTION 35

You have a data loss prevention (DLP) policy configured for endpoints as shown in the following exhibit.



From a computer named Computer1, a user can sometimes upload files to cloud services and sometimes cannot. Other users experience the same issue.

What are two possible causes of the issue? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. The computers are NOT onboarded to the Microsoft 365 compliance center.
- B. The Copy to clipboard action is set to Audit only.
- C. There are file path exclusions in the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings.
- D. The Access by unallowed apps action is set to Audit only.
- E. The unallowed browsers in the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings are NOT configured.

Correct Answer: D, E

Section:

02 - Implement Data Loss Prevention

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the

scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

Overview

Fabrikam, Inc. is a consulting company that has a main office in Montreal and six branch offices in New York, Seattle, Miami, Houston, Los Angeles, and Vancouver.

Existing Environment

Cloud Environment

Fabrikam has a Microsoft 365 tenant that contains the following resources:

An on-premises Active Directory domain named corp.fabrikam.com that syncs to an Azure Active Directory (Azure AD) tenant

Microsoft Cloud App Security connectors configured for all supported cloud applications used by the company

Some users have company Dropbox accounts.

Compliance Configuration

Fabrikam has the following in the Microsoft 365 compliance center:

A data loss prevention (DLP) policy is configured. The policy displays a tooltip to users. Users can provide a business justification to override a DLP policy violation.

The Azure Information Protection unified labeling scanner is installed and configured.

A sensitivity label named Fabrikam Confidential is configured.

An existing third-party records management system is managed by the compliance department.

Human Resources (HR) Management System

The HR department has an Azure SQL database that contains employee information. Each employee has a unique 12-character alphanumeric ID. The database contains confidential employee attributes including payroll information, date of birth, and personal contact details.

On-Premises Environment

You have an on-premises file server that runs Windows Server 2019 and stores Microsoft Office documents in a shared folder named Data.

All end-user computers are joined to the corp.fabrikam.com domain and run a third-party antimalware application.

Business Processes

Sales Contracts

Users in the sales department receive draft sales contracts from customers by email. The sales contracts are written by the customers and are not in a standard format.

Employment Applications

Employment applications and resumes are received by HR department managers and stored in either mailboxes, Microsoft SharePoint Online sites, OneDrive for Business folders, or Microsoft Teams channels.

The employment application form is downloaded from SharePoint Online and a serial number is assigned to each application.

The resumes are written by the applicants and are in any format.

Requirements

HR Requirements

You need to create a DLP policy that will notify the HR department of a DLP policy violation if a document that contains confidential employee attributes is shared externally. The DLP policy must use an Exact Data Match (EDM) classification derived from a CSV export of the HR department database.

The HR department identifies the following requirements for handling employment applications:

Resumes must be identified automatically based on similarities to other resumes received in the past.

Employment applications and resumes must be deleted automatically two years after the applications are received.

Documents and emails that contain an application serial number must be identified automatically and marked as an employment application.

Sales Requirements

A sensitivity label named Sales Contract must be applied automatically to all draft and finalized sales contracts.

Compliance Requirements

Fabrikam identifies the following compliance requirements:

All DLP policies must be applied to computers that run Windows 10, with the least possible changes to the computers.

Users in the compliance department must view the justification provided when a user receives a tooltip notification for a DLP violation.

If a document that has the Fabrikam Confidential sensitivity label applied is uploaded to Dropbox, the file must be deleted automatically.

The Fabrikam Confidential sensitivity label must be applied to existing Microsoft Word documents in the Data shared folder that have a document footer containing the following string: Company use only.

Users must be able to manually select that email messages are sent encrypted. The encryption will use Office 365 Message Encryption (OME) v2. Any email containing an attachment that has the Fabrikam Confidential sensitivity label applied must be encrypted automatically by using OME.

Existing policies configured in the third-party records management system must be replaced by using Records management in the Microsoft 365 compliance center. The compliance department plans to export the existing policies, and then produce a CSV file that contains matching labels and policies that are compatible with records management in Microsoft 365. The CSV file must be used to configure records management in Microsoft 365. Executive Requirements

You must be able to restore all email received by Fabrikam executives for up to three years after an email is received, even if the email was deleted permanently.

QUESTION 1

You need to recommend a solution that meets the compliance requirements for viewing DLP tooltip justifications. What should you recommend?

- A. Instruct the compliance department users to review the False positive and override report.
- B. Configure a Microsoft Power Automate workflow to route DLP notification emails to the compliance department.
- C. Instruct the compliance department users to review the DLP incidents report.
- D. Configure an Azure logic app to route DLP notification emails to the compliance department.

Correct Answer: A

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/view-the-dlp-reports?view=o365-worldwide>

QUESTION 2

You need to recommend a solution that meets the compliance requirements for Dropbox. What should you recommend?



- A. Create a file policy in Cloud App Security that uses the built-in DLP inspection method.
- B. Edit an existing retention label that enforces the item deletion settings.
- C. Create a retention label that enforces the item deletion settings.
- D. Create a DLP policy that applies to devices.

Correct Answer: A

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-use-policies-non-microsoft-cloud-apps?view=o365-worldwide>

QUESTION 3

You need to implement a solution that meets the compliance requirements for the Windows 10 computers. Which two actions should you perform? Each correct answer presents part of the solution. (Choose two.)
NOTE: Each correct selection is worth one point.

- A. Deploy a Microsoft 365 Endpoint data loss prevention (Endpoint DLP) configuration package to the computers.
- B. Configure the Microsoft Intune device enrollment settings.
- C. Configure hybrid Azure AD join for all the computers.
- D. Configure a compliance policy in Microsoft Intune.
- E. Enroll the computers in Microsoft Defender for Endpoint protection.

Correct Answer: C, E

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started?view=o365-worldwide>

QUESTION 4

You need to recommend a solution to configure the Microsoft 365 Records management settings by using the CSV file. The solution must meet the compliance requirements. What should you recommend?

- A. Use EdmUploadAgent.exe to upload a hash of the CSV to a data store.
- B. Use a PowerShell command that pipes the Import-Csv cmdlet to the New-RetentionPolicy cmdlet.
- C. From the Microsoft 365 compliance center, import the CSV file to a file plan.
- D. Use a PowerShell command that pipes the Import-Csv cmdlet to the New-Label cmdlet.

Correct Answer: C

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/file-plan-manager?view=o365-worldwide#import-retention-labels-into-your-file-plan>

03 - Implement Data Loss Prevention

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click 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.



QUESTION 1

You are evaluating the technical requirements for the DLP reports.
Which user can currently view the DLP reports?

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

Correct Answer: E
Section:

QUESTION 2

HOTSPOT

How many files in Site2 will be visible to User1 and User2 after you turn on DLPpolicy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

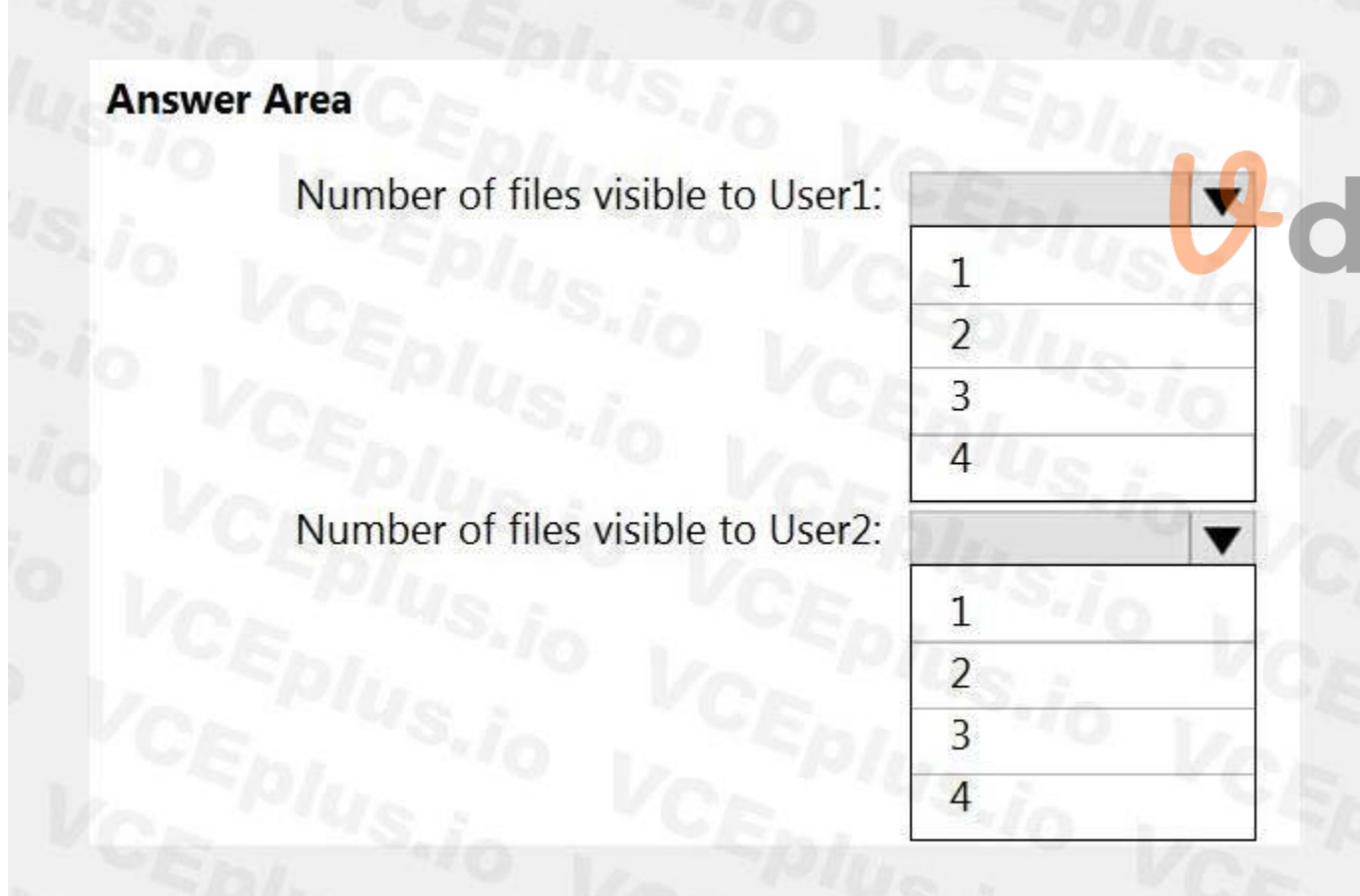
Answer Area

Number of files visible to User1:

▼
1
2
3
4

Number of files visible to User2:

▼
1
2
3
4



Answer Area:

Answer Area

Number of files visible to User1:

▼
1
2
3
4

Number of files visible to User2:

▼
1
2
3
4

Section:

Explanation:

Reference:

<https://social.technet.microsoft.com/wiki/contents/articles/36527.implement-data-loss-prevention-dlp-in-sharepoint-online.aspx>



01 - Implement Information Governance

QUESTION 1

HOTSPOT

You have the files shown in the following table.

Name	Location	Date modified	Date created
File1	Microsoft SharePoint Online site	June 01, 2018	December 28, 2011
File2	Microsoft OneDrive account	February 02, 2017	January 02, 2011
File3	Microsoft Exchange Online public folder	May 01, 2006	May 01, 2006

You configure a retention policy as shown in the exhibit.

RetentionPolicy 1

Status

Enabled (Pending)

Policy name

RetentionPolicy1

Description

RetentionPolicy1

Applies to content in these locations

SharePoint sites

Settings

Retention period

Keep content, and delete it if it's older than 7 years

Preservation lock

No data available

The start of the retention period is based on when items are created. The current date is January 01, 2021.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
File1 will be deleted after you turn on the policy.	<input type="radio"/>	<input type="radio"/>
File2 will be deleted after you turn on the policy.	<input type="radio"/>	<input type="radio"/>
File3 will be deleted after you turn on the policy.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Statements	Yes	No
File1 will be deleted after you turn on the policy.	<input checked="" type="radio"/>	<input type="radio"/>
File2 will be deleted after you turn on the policy.	<input type="radio"/>	<input checked="" type="radio"/>
File3 will be deleted after you turn on the policy.	<input type="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-sharepoint?view=o365-worldwide>

QUESTION 2

You create a retention label that has a retention period of seven years.

You need to ensure that documents containing a credit card number are retained for seven years. Other documents must not be retained.

What should you create?

- A. a retention label policy of type publish
- B. a retention policy that retains file automatically
- C. a retention policy that deletes files automatically
- D. a retention label policy of type auto-apply

Correct Answer: D

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-retention-labels-automatically?view=o365-worldwide>

QUESTION 3

You have a Microsoft 365 E5 tenant that contains a user named User1.
You need to identify the type and number of holds placed on the mailbox of User1.
What should you do first?

- A. From the Microsoft 365 compliance center, create an eDiscovery case.
- B. From Exchange Online PowerShell, run the Get-Mailbox cmdlet.
- C. From the Microsoft 365 compliance center, run a content search.
- D. From Exchange Online PowerShell, run the Get-HoldCompliancePolicy cmdlet

Correct Answer: B

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/identify-a-hold-on-an-exchange-onlinemailbox?view=o365-worldwide>

QUESTION 4

HOTSPOT

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

Name	Role
User1	Global Administrator
User2	Compliance admin

The logo for Vdumps.com, featuring a stylized orange 'V' followed by the word 'dumps' in a grey, lowercase sans-serif font.

You have a retention policy that has the following configurations:

Name: Policy1

Retain items for a specific period: 5 years

Locations to apply the policy: Exchange email, SharePoint sites

You place a Preservation Lock on Policy1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Statements	Yes	No
User1 can remove Exchange email from the locations	<input type="radio"/>	<input type="radio"/>
User2 can increase the retention period to seven years	<input type="radio"/>	<input type="radio"/>
User1 can decrease the retention period to three years	<input type="radio"/>	<input type="radio"/>

Answer Area:

Statements	Yes	No
User1 can remove Exchange email from the locations	<input type="radio"/>	<input checked="" type="radio"/>
User2 can increase the retention period to seven years	<input checked="" type="radio"/>	<input type="radio"/>
User1 can decrease the retention period to three years	<input type="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

When a retention policy is locked:

No one, including the global admin, can disable the policy or delete it

Locations can be added but not removed

You can extend the retention period but not decrease it

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-preservation-lock?view=o365worldwide>

QUESTION 5

HOTSPOT

You have a Microsoft E5 365 tenant.

You need to ensure that you can use sensitivity labels to declare regulatory records.

Which PowerShell cmdlet should you run, and which type of policy should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Cmdlet:

	▼
Set-RetentionCompliancePolicy	
Set-RegulatoryComplianceUI	
Set-RetentionPolicyTag	

Policy type:

	▼
Auto-labeling policy	
Retention label policy	
Retention policy	

Answer Area:

Answer Area

Cmdlet:

	▼
Set-RetentionCompliancePolicy	
Set-RegulatoryComplianceUI	
Set-RetentionPolicyTag	

Policy type:

	▼
Auto-labeling policy	
Retention label policy	
Retention policy	

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/declare-records?view=o365-worldwide>
<https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-sensitivity-labels?view=o365-worldwide>

QUESTION 6

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

Name	Role
User1	Global administrator
User2	Security administrator
User3	Compliance administrator
User4	Search administrator

You configure a retention label to trigger a disposition review at the end of the retention period.

Which users can access the Disposition tab in the Microsoft 365 compliance center to review the content?

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

E. User3 and User4

Correct Answer: C

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide>

QUESTION 7

You need to ensure that documents in a Microsoft SharePoint Online site that contain a reference to Project Alpha are retained for two years, and then deleted.

Which two objects should you create? Each correct answer presents part of the solution. (Choose two.)

NOTE: Each correct selection is worth one point.

- A. a retention policy
- B. an auto-apply label policy
- C. a sensitive info type
- D. a retention label
- E. a sensitivity label
- F. a publishing label policy

Correct Answer: B, D

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-retention-labels-automatically?view=o365-worldwide>

QUESTION 8

You are configuring a retention label named Label1 as shown in the following exhibit.



Define retention settings

When this label is applied to items, the content is retained and/or deleted based on the settings you choose here.

Retain items for a specific period

Labeled items will be retained for the period you choose. During the retention period, Users will be able to edit items and change or remove the label. If they delete items, we'll keep copies in a secure location. [Learn more](#)

Retention period of years months days

Start the retention period based on

+ Create new event type

At the end of the retention period

Delete items automatically

We'll delete items from where they're currently stored.

Trigger a disposition review

Do nothing

Items will be left in place. You'll have to manually delete them if you want them gone.

Retain items forever

Labeled items will be retained forever, even if users delete them. Users will be able to edit items and change or remove the label. If they delete items, we'll keep copies in a secure location. [Learn more](#)

Only delete items when they reach a certain age

Labeled items won't be retained, but when they reach the age you choose, we'll delete them from where they're stored.

You need to ensure that documents that have Label1 applied are deleted three years after the end of your company's fiscal year. What should you do?

- A. Create a new event type.
- B. Select Only delete items when they reach a certain age.
- C. Modify the Retention period setting.
- D. Set At the ends of the retention period to Trigger a disposition review.

Correct Answer: A

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/event-driven-retention?view=o365-worldwide>

QUESTION 9

You have a Microsoft 365 tenant.

You have a Microsoft SharePoint Online site that contains employment contracts in a folder named EmploymentContracts. All the files in EmploymentContracts are marked as records.

You need to recommend a process to ensure that when a record is updated, the previous version of the record is kept as a version of the updated record.

What should you recommend?

- A. Upload an updated file plan that contains the record definition.
- B. Unlock the record, modify the record, and then lock the record.
- C. Create a copy of the record and enter a version in the file metadata.
- D. Create a new label policy associated to an event that will apply to the record.

Correct Answer: B

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/record-versioning?view=o365-worldwide>

QUESTION 10

You have a Microsoft 365 tenant.

All Microsoft OneDrive for Business content is retained for five years.

A user named User1 left your company a year ago, after which the account of User1 was deleted from Azure Active Directory (Azure AD).

You need to recover an important file that was stored in the OneDrive of User1.

What should you use?

- A. the Restore-SPODeletedSite PowerShell cmdlet
- B. the OneDrive recycle bin
- C. the Restore-ADObject PowerShell cmdlet
- D. Deleted users in the Microsoft 365 admin center



Correct Answer: B

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/onedrive/set-retention> <https://docs.microsoft.com/en-us/onedrive/retention-and-deletion>

QUESTION 11

At the end of a project, you upload project documents to a Microsoft SharePoint Online library that contains many files. The following is a sample of the project document file names:

aei_AA989.docx

bci_WS098.docx

cei_DF112.docx

ebc_QQ454.docx

ecc_BB565.docx

All documents that use this naming format must be labeled as Project Documents:

You need to create an auto-apply retention label policy.

What should you use to identify the files?

- A. A sensitive info type
- B. A retention label
- C. A trainable classifier

Correct Answer: C

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide>

QUESTION 12

You need to create a retention policy to retain all the files from Microsoft Teams channel conversations and private chats. Which two locations should you select in the retention policy? Each correct answer presents part of the solution.

(Choose two.)

NOTE: Each correct selection is worth one point.

- A. OneDrive accounts
- B. Office 365 groups
- C. Team channel messages
- D. SharePoint sites
- E. Team chats
- F. Exchange email

Correct Answer: A, D

Section:

Explanation:

Reference: <https://support.microsoft.com/en-us/office/file-storage-in-teams-df5cc0a5-d1bb-414c-8870-46c6eb76686a>

QUESTION 13

You have a Microsoft 365 tenant that uses records management.

You use a retention label to mark legal files stored in a Microsoft SharePoint Online document library as regulatory records.

What can you do to the legal files?

- A. Rename the files.
- B. Edit the properties of the files.
- C. Change the retention label of the files.
- D. Copy the content of the files.

Correct Answer: D

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/records-management?view=o365-worldwide>

QUESTION 14

DRAG DROP

You have a Microsoft 365 tenant.

A new regulatory requirement states that all documents containing a patent ID be labeled, retained for 10 years, and then deleted. The policy used to apply the retention settings must never be disabled or deleted by anyone.

You need to implement the regulatory requirement.

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. (Choose three.)

Select and Place:

Actions

- Create a retention policy.
- Add a preservation lock.
- Add a management lock.
- Create a retention label.
- Create a retention label policy.

Answer Area

Correct Answer:

Actions

- Create a retention policy.
-
- Add a management lock.
-
-

Answer Area

- Create a retention label.
- Create a retention label policy.
- Add a preservation lock.

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide>

<https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-preservation-lock?view=o365-worldwide>

QUESTION 15

HOTSPOT

You create a retention policy as shown in the following exhibit.

Retention Policy 1

Status

Enabled (Pending)

Policy name

Retention Policy 1

Description

Retention Policy for SharePoint Site1 and Exchange

Applies to content in these locations

Exchange email

SharePoint sites

Settings

Retention period

Keep content, and delete it if it's older than 10 years

Preservation lock

No data available

A user named User1 deletes a file named File1.docx from a Microsoft SharePoint Online site named Site1.

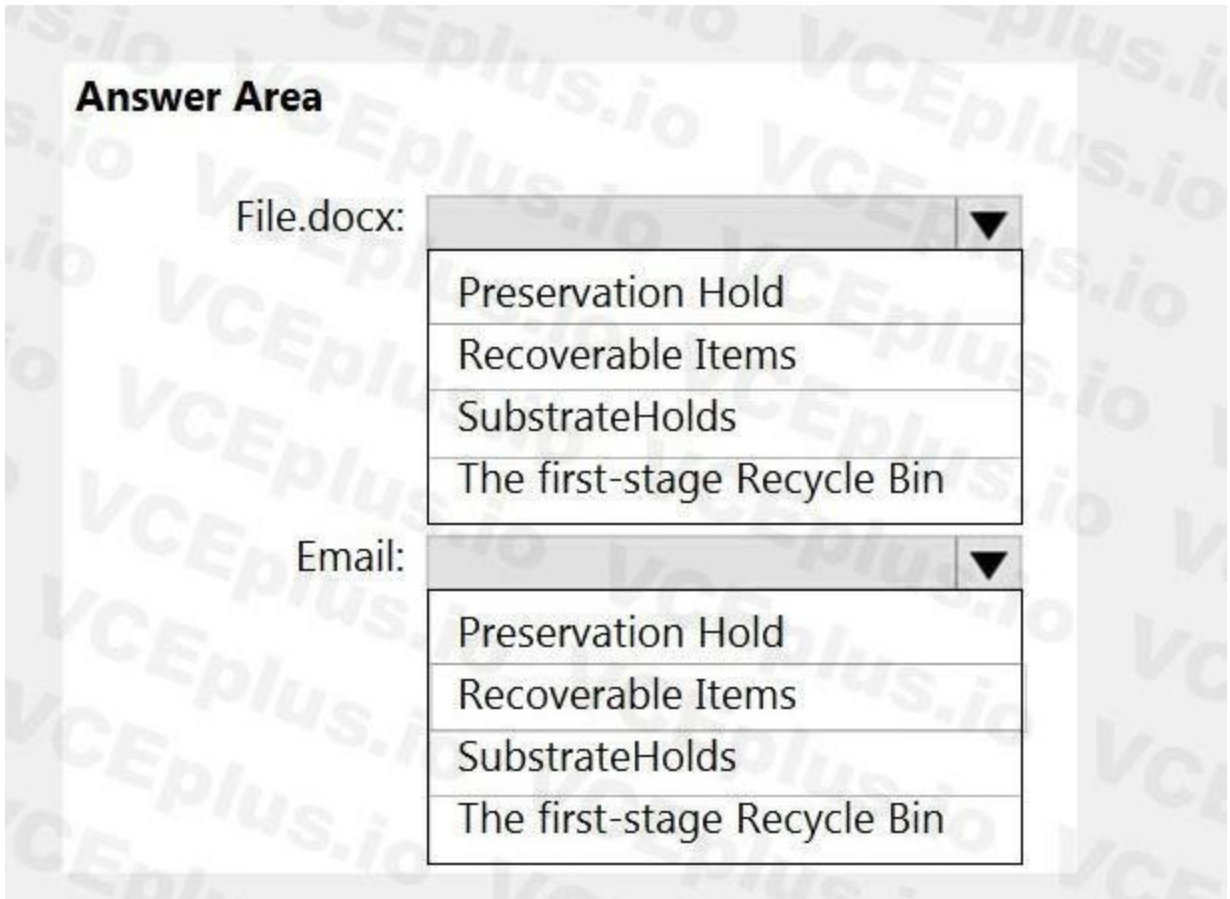
A user named User2 deletes an email and empties the Deleted Items folder in Microsoft Outlook.

Where is the content retained one year after deletion? To answer, select the appropriate options in the answer area.

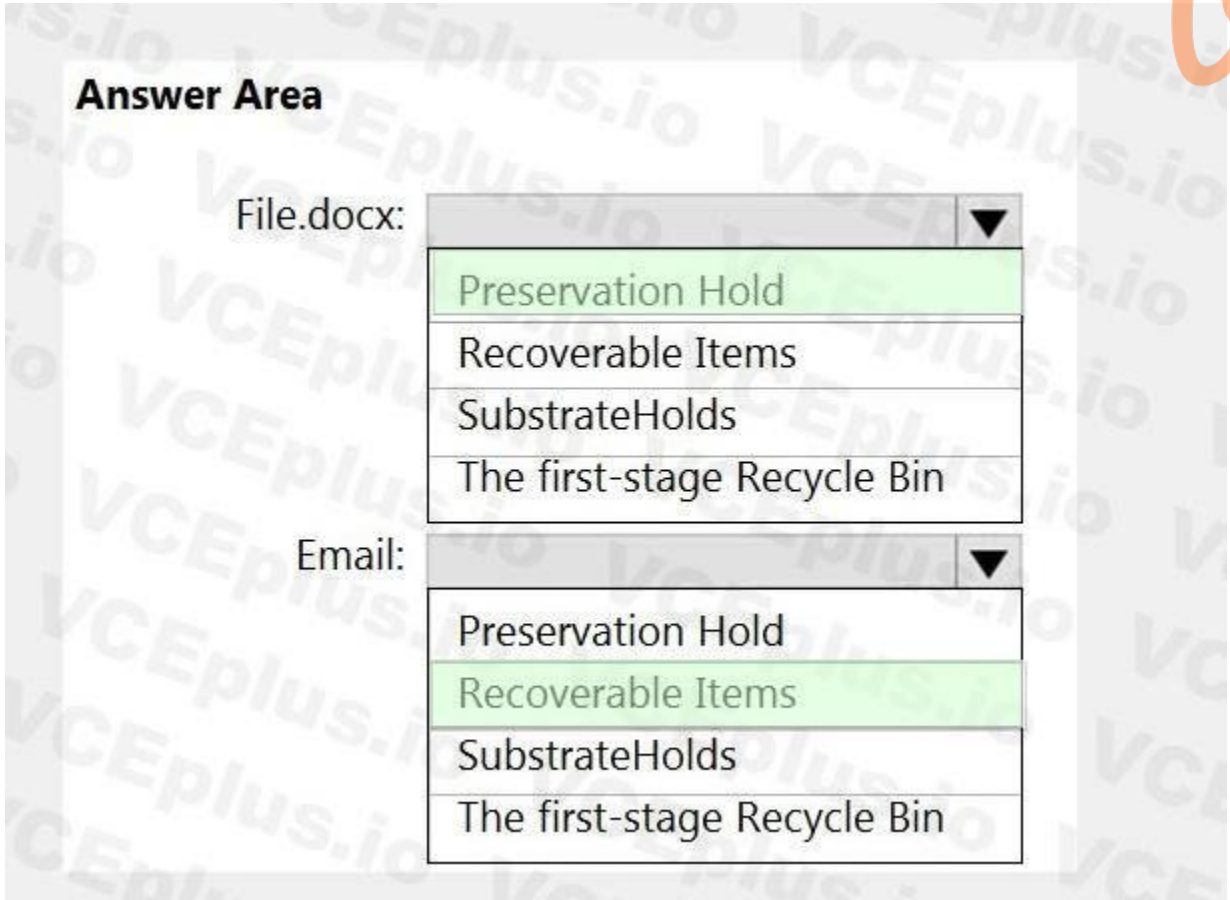
NOTE: Each correct selection is worth one point.

Hot Area:





Answer Area:



Section:
Explanation:



Reference:
<https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide>

QUESTION 16

DRAG DROP
You have a Microsoft 365 tenant.
A new regulatory requirement states that all documents containing a patent ID be labeled, retained for 10 years, and then deleted. The policy used to apply the retention settings must never be disabled or deleted by anyone.
You need to implement the regulatory requirement.
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. (Choose three.)

Select and Place:

Actions	Answer Area
Add a management lock.	
Create a retention label policy.	
Add a preservation lock.	
Create a retention policy.	
Create a retention label.	

Correct Answer:

Actions	Answer Area
Add a management lock.	Create a retention label.
	Create a retention label policy.
	Add a preservation lock.
Create a retention policy.	

Section:
Explanation:
Reference:
<https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide>

QUESTION 17

HOTSPOT
You create a retention label policy named Contoso_Policy that contains the following labels:
10 years then delete 5 years then delete
Do not retain

Contoso_Policy is applied to content in Microsoft SharePoint Online sites.

After a couple of days, you discover the following messages on the Properties page of the label policy:

Status: Off (Error)

It's taking longer than expected to deploy the policy

You need to reinitiate the policy.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.


Hot Area:

Answer Area

	-id Contoso_Policy	
Set-RetentionCompliancePolicy		-ForceFullSync
Set-RetentionPolicy		-FullCrawl
Start-EdgeSynchronization		-RetryDistribution
Start-RetentionAutoTagLearning		-Train

Answer Area:

Answer Area



	-id Contoso_Policy	
Set-RetentionCompliancePolicy		-ForceFullSync
Set-RetentionPolicy		-FullCrawl
Start-EdgeSynchronization		-RetryDistribution
Start-RetentionAutoTagLearning		-Train

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/powershell/module/exchange/set-retentioncompliancepolicy?view=exchange-ps>

QUESTION 18

HOTSPOT

You have a Microsoft 365 tenant.

A retention hold is applied to all the mailboxes in Microsoft Exchange Online.

A user named User1 leaves your company, and the account of User1 is deleted from Azure Active Directory (Azure AD).

You need to create a new user named User2 and provide User2 with access to the mailbox of User1.

How should you complete the PowerShell command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
$InactiveMailbox = Get-Mailbox -InactiveMailboxOnly -Identity <distinguished name>
```

	▼	▼	\$InactiveMailbox.DistinguishedName
New-Mailbox		-InactiveMailbox	
New-MailboxRestoreRequest		-LitigationHoldEnabled	
Restore-RecoverableItems		-RetentionHoldEnabled	
Set-Mailbox		-SourceMailbox	

```
-Name User2 -DisplayName User2 -MicrosoftOnlineServicesID user2@contoso.com  
-Password (ConvertTo-SecureString -String 'RdFGFfhjjhgff$^^7' -AsPlainText -Force)  
-ResetPasswordOnNextLogon $true
```

Answer Area:

Answer Area

```
$InactiveMailbox = Get-Mailbox -InactiveMailboxOnly -Identity <distinguished name>
```

	▼	▼	\$InactiveMailbox.DistinguishedName
New-Mailbox		-InactiveMailbox	
New-MailboxRestoreRequest		-LitigationHoldEnabled	
Restore-RecoverableItems		-RetentionHoldEnabled	
Set-Mailbox		-SourceMailbox	

```
-Name User2 -DisplayName User2 -MicrosoftOnlineServicesID user2@contoso.com  
-Password (ConvertTo-SecureString -String 'RdFGFfhjjhgff$^^7' -AsPlainText -Force)  
-ResetPasswordOnNextLogon $true
```

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/recover-an-inactive-mailbox?view=o365-worldwide>

QUESTION 19

Your company manufactures parts that are each assigned a unique 12-character alphanumeric serial number. Emails between the company and its customers reference the serial number.

You need to ensure that only Microsoft Exchange Online emails containing the serial numbers are retained for five years.

Which three objects should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a sensitivity label
- B. a retention policy
- C. an auto-labeling policy
- D. a trainable classifier
- E. a sensitive info type
- F. a retention label
- G. a data loss prevention (DLP) policy

Correct Answer: C, E, F

Section:

Explanation:

C: One of the most powerful features of retention labels is the ability to apply them automatically to content that matches specified conditions.

F: You can apply retention labels to content automatically when that content contains:

Specific types of sensitive information

Specific keywords or searchable properties that match a query you create

A match for trainable classifiers

E: Sensitive information types are pattern-based classifiers. They detect sensitive information like social security, credit card, or bank account numbers to identify sensitive items. Custom sensitive information types use regular expressions, keywords, and keyword dictionaries.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitive-information-type-learn-about?view=o365-worldwide>

<https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide>

<https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide>



QUESTION 20

You plan to import a file plan to the Microsoft 365 compliance center.

Which object type can you create by importing a records management file plan?

- A. retention label policies
- B. sensitive info types
- C. sensitivity labels
- D. retention labels

Correct Answer: A

Section:

QUESTION 21

HOTSPOT

You have a Microsoft 365 tenant that uses a domain named contoso.com.

A user named User1 leaves your company. The mailbox of User1 is placed on Litigation Hold, and then the account of User1 is deleted from Azure Active Directory (Azure AD).

You need to copy the content of the User1 mailbox to a folder in the existing mailbox of another user named User2.

How should you complete the PowerShell command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
$InactiveMailbox = Get-Mailbox -InactiveMailboxOnly -Identity <distinguished name>
```

	\$InactiveMailbox.DistinguishedName
New-Mailbox	-InactiveMailbox
New-MailboxRestoreRequest	-LitigationHoldEnabled
Restore-RecoverableItems	-RetentionHoldEnabled
Set-Mailbox	-SourceMailbox

```
-TargetMailbox user2@contoso.com -TargetRootFolder "User1 Mailbox"
```

Answer Area:

Answer Area

```
$InactiveMailbox = Get-Mailbox -InactiveMailboxOnly -Identity <distinguished name>
```

	\$InactiveMailbox.DistinguishedName
New-Mailbox	-InactiveMailbox
New-MailboxRestoreRequest	-LitigationHoldEnabled
Restore-RecoverableItems	-RetentionHoldEnabled
Set-Mailbox	-SourceMailbox

```
-TargetMailbox user2@contoso.com -TargetRootFolder "User1 Mailbox"
```

Section:

Explanation:

References:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/restore-an-inactive-mailbox?view=o365-worldwide>

QUESTION 22

HOTSPOT

While creating a retention label, you discover that the following options are missing:

Mark items as a record

Mark items as a regulatory record

You need to ensure that the options are available when you create retention labels in the Microsoft 365 compliance center.
How should you complete the PowerShell script? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
$UserCredential = Get-Credential
```

Import-Module


AzureRM
ExchangeOnlineManagement
Microsoft.Online.SharePoint.PowerShell
MicrosoftTeams

-Credential \$UserCredential

Connect-AadrmService
Connect-AzureAD
Connect-AzureRMAccount
Connect-IPPSSession

-Enabled \$true

Enable-ComplianceTagStorage
New-ComplianceTag
Set-RegulatoryComplianceUI
Set-RetentionCompliancePolicy



Answer Area:

Answer Area

```
$UserCredential = Get-Credential
```

```
Import-Module
```

AzureRM
ExchangeOnlineManagement
Microsoft.Online.SharePoint.PowerShell
MicrosoftTeams

```
-Credential $UserCredential
```

Connect-AadrmService
Connect-AzureAD
Connect-AzureRMAccount
Connect-IPPSSession

```
-Enabled $true
```

Enable-ComplianceTagStorage
New-ComplianceTag
Set-RegulatoryComplianceUI
Set-RetentionCompliancePolicy



Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/declare-records?view=o365-worldwide>

<https://docs.microsoft.com/en-us/powershell/exchange/connect-to-scc-powershell?view=exchange-ps>

QUESTION 23

HOTSPOT

You enable archive mailboxes for all the users at your company.

The Default MRM Policy is shown in the MRM exhibit.

Default MRM Policy

This policy contains the following retention tags

1 Month Delete

1 Week Delete

1 Year Delete

5 Year Delete

6 Month Delete

Default 2 year move to archive

Junk Email

Never Delete

Personal 1 year move to archive

Personal 5 year move to archive

Personal never move to archive

Recoverable items 14 days move to archive

A Microsoft 365 retention label policy is shown in the Label Policy exhibit.



Exchange Label Policy

Status

Enabled (Pending)

Policy name

Exchange Label Policy

Description

Label policy for Exchange

Applies to content in these locations

Exchange email

Settings

Publish labels for your users

- 10 Year – Do not Delete
- 2 Year Delete

Preservation lock

No

You need to identify the following:

How many years until an email is archived?

What should you modify to change the retention period for archiving?

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

By default, email is:

Deleted after two years
Deleted after one month
Retained in the mailbox for 10 years
Moved to the archive mailbox after two years

To change the retention period for archiving, modify:

The Default MRM Policy
The Exchange Label Policy
The properties of the archive mailbox

Answer Area:



Answer Area

By default, email is:

Deleted after two years
Deleted after one month
Retained in the mailbox for 10 years
Moved to the archive mailbox after two years

To change the retention period for archiving, modify:

The Default MRM Policy
The Exchange Label Policy
The properties of the archive mailbox

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide#the-principles-of-retention-or-what-takes-precedence>

02 - Implement Information Governance

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click 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.



QUESTION 1

You need to meet the retention requirement for the users' Microsoft 365 data.

What is the minimum number of retention policies that you should use?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 6

Correct Answer: A

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide>

QUESTION 2

HOTSPOT

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.

Hot 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 type="radio"/>	<input type="radio"/>
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="radio"/>	<input type="radio"/>
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="radio"/>	<input type="radio"/>

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="radio"/>	<input type="radio"/>
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 checked="" type="radio"/>	<input type="radio"/>
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="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide>

Exam F

QUESTION 1

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 compliance 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-AuditConfig -Workload Exchange command.

Does that meet the goal?

A. Yes

B. No

Correct Answer: A

Section:

QUESTION 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 compliance portal to identify who signed in to the mailbox of User1, the result 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

Correct Answer: B

Section:

QUESTION 3

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 E5 subscription.

You need to identify resumes that are stored in the subscription by using a built-in trainable classifier.

Solution: You create an auto-labeling policy for a retention label.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

QUESTION 4

HOTSPOT

You have a Microsoft 365 subscription that contains two groups named Group1 and Group2.

You have the compliance assessments shown in the following table.

Name	Group
Ca1	Group1
Ca2	Group1
Ca3	Group2

You have the improvement actions shown in the following table.

Action	Compliance assessment	Improvement action	Points	Action type
Action1	Ca1	Create and publish a retention label	5	Technical
Action2	Ca2	Create and publish a retention label	5	Technical
Action3	Ca3	Enable Windows 10 Security baseline	5	Technical
Action4	Ca1	Restrict access to privileged accounts	10	Operational
Action5	Ca2	Update security awareness training	10	Operational
Action6	Ca3	Update security awareness training	10	Operational

You perform the following actions:

- * Create and publish a retention label.
- * Implement security awareness training for all users.
- * For Action4, change Implementation status to Implemented

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
The compliance score for Ca1 will increase by 15 points.	<input type="radio"/>	<input type="radio"/>
The compliance score for Ca2 will increase by 15 points.	<input type="radio"/>	<input type="radio"/>
The compliance score for Ca3 will increase by 10 points.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
The compliance score for Ca1 will increase by 15 points.	<input checked="" type="radio"/>	<input type="radio"/>
The compliance score for Ca2 will increase by 15 points.	<input type="radio"/>	<input checked="" type="radio"/>
The compliance score for Ca3 will increase by 10 points.	<input checked="" type="radio"/>	<input type="radio"/>

Section:

Explanation:

QUESTION 5

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a user named User1 and the groups shown in the following table.

Name	Type
Group1	Microsoft 365
Group2	Security

You have the Compliance Manager improvement action shown in the following exhibit

E Enable self-service password reset

Overview

Details

Implementation Status Not Implemented	Test Status Failed high risk
Points achieved 0 / 27	Group Default Group
Managed by Your organization	Action scope Tenant
Action type Technical	Products Microsoft 365

Edit implementation details

How to implement

technical Microsoft 365

Documents

0

Assigned to

None

Assign action

Testing Source

Manual

Implementation Testing Standards and Regulations Documents

Implementation status

● Not Implemented

Implementation date

Not Available

Implementation notes

This action hasn't been implemented yet. Refer to the implementation instructions for this action.

Edit implementation details

How to implement

Microsoft recommends that your organization enable self-service password reset to allow users who have either forgotten their password or whose account has been locked out as a result of malicious attempts, using an alternate factor to reset their password without the assistance of the help desk.

How to Use Microsoft Solutions to Implement

Your organization can use Azure Active Directory (Azure AD) to give users the ability to change or reset their password with no administrator or help desk involvement. Select **Launch Now** to enable Self-Service Password Reset (SSPR) by selecting "All" or "Selected" on the "Properties" page to determine applicable users.

[Launch Now](#)

Learn More

[Let users reset their own passwords in Office 365](#)

[How it works: Azure Active Directory self-service password reset](#)

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.

Hot Area:

Answer Area

The Enable self-service password reset improvement action can be assigned to **[answer choice]**.

▼

- User1 only
- Group1 only
- User1 and Group1 only
- Group1 and Group2 only
- User1, Group1, and Group2

Twenty-four hours after self-service password reset (SSPR) is enabled for all users, Points achieved will be **[answer choice]**.

▼

- 0/27
- 1/27
- 2/27
- 5/27
- 27/27

Answer Area:

Answer Area

The Enable self-service password reset improvement action can be assigned to **[answer choice]**.

▼

- User1 only
- Group1 only
- User1 and Group1 only
- Group1 and Group2 only
- User1, Group1, and Group2

Twenty-four hours after self-service password reset (SSPR) is enabled for all users, Points achieved will be **[answer choice]**.

▼

- 0/27
- 1/27
- 2/27
- 5/27
- 27/27

Section:

Explanation:

QUESTION 6

HOTSPOT

You have a Microsoft 365 ES subscription.

You plan to create a custom trainable classifier by uploading 1,000 machine-generated files as seed content.


The files have sequential names and are uploaded in one-minute intervals as shown in the following table.

Number	Name	Upload time
1	File001.docx	3:01 AM
2	File002.docx	3:02 AM
3	File003.docx	3:03 AM
<i>994 rows not shown</i>		
998	File998.docx	7:38 PM
999	File999.docx	7:39 PM
1000	File000.docx	7:40 PM


Which files were processed first and last when you created the custom trainable classifier? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

First: 


- File001.docx
- File301.docx
- File501.docx
- File801.docx
- File951.docx

Last: 


- File050.docx
- File200.docx
- File300.docx
- File500.docx
- File000.docx

Answer Area:

Answer Area

First: 

- File001.docx
- File301.docx
- File501.docx
- File801.docx
- File951.docx

Last: 

- File050.docx
- File200.docx
- File300.docx
- File500.docx
- File000.docx

Section:

Explanation:

QUESTION 7

HOTSPOT

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

Name	Email address	Distribution group
User1	user1@contoso.com	Finance
User2	user2@contoso.com	Sales

You create the data loss prevention (DLP) policies shown in the following table.

Name	Order	Apply policy to	Conditions	Actions	Exceptions	User notifications	Additional options
Policy1	0	Exchange email for the Finance distribution group	Content shared with people outside my organization. Content contains five or more credit card numbers.	Encrypt the message by using the Encrypt email messages option.	user4@fabrikam.com	Send an incident report to the administrator.	If there's a match for this rule, stop processing additional DLP policies and rules.
Policy2	1	All locations of Exchange email	Content shared with people outside my organization. Content contains five or more credit card numbers.	Restrict access or encrypt the content in Microsoft 365 locations. Block only people outside your organization.	None	Send an incident report to the administrator.	None

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements

If User1 sends an email message that contains five credit card numbers to user4@fabrikam.com, the message will be encrypted.

If User1 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered.

If User2 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered.

Yes	No
<input type="radio"/>	<input type="radio"/>
<input checked="" type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements

If User1 sends an email message that contains five credit card numbers to user4@fabrikam.com, the message will be encrypted.

If User1 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered.

If User2 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered.

Yes	No
<input type="radio"/>	<input checked="" type="radio"/>
<input checked="" type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

QUESTION 8

You have a Microsoft 365 E5 subscription.

You create a role group named Role1.

You need to add a role to Role1 that will enable group members to view the metadata of records that were tagged for deletion automatically at the end of the records' retention period. The solution must use the principle of least privilege.

Which role should you add?

- A. Review
- B. View-Only Retention Management
- C. Retention Management
- D. Disposition Management
- E. Record Management

Correct Answer: B
Section:

QUESTION 9
HOTSPOT

You have a Microsoft 365 ES subscription that uses data loss prevention (DLP) to protect sensitive information.

You need to create scheduled reports that generate.

* DLP policy matches reported over the shortest frequency of time

* DLP incidents reported over the longest frequency of time

Which frequency should you configure for each report? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

DLP policy matches: Daily

- Daily
- Every two days
- Weekly
- Every two weeks
- Monthly

DLP incidents: Monthly

- Weekly
- Every two weeks
- Monthly
- Every three months
- Every six months

Answer Area:

Answer Area

DLP policy matches: Daily

- Daily
- Every two days
- Weekly
- Every two weeks
- Monthly

DLP incidents: Monthly

- Weekly
- Every two weeks
- Monthly
- Every three months
- Every six months

Section:

Explanation:

QUESTION 10

HOTSPOT

You have a Microsoft 365 E5 subscription.

You receive the data loss prevention (DIP) alert shown in the following exhibit.

The screenshot shows a Microsoft Purview alert interface for Contoso Electronics. The alert title is "Sensitive info in email with subject 'Message1'". The interface includes tabs for "Details", "Sensitive info types", and "Metadata".

Event details

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

Time of activity
Jun 6, 2022 8:22 PM

Impacted entities

User	Email recipients
Megan Bowen	victoria@fabrikam.com

Email subject
Message1

Policy details

DLP policy matched	Rule matched
Policy1	Rule1
Sensitive info types detected	Actions taken
Credit Card Number (19, 85%)	GenerateAlert
User override policy	Override justification text
Yes	Manager approved

Sensitive info detected in
Document1.docx



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graph.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The email was [answer choice].

- sent to a manager for approval
- delivered immediately
- quarantined and undelivered
- sent to a manager for approval

The sender's manager [answer choice].

- override Rule1
- approved the email by using a workflow
- override Rule1
- was uninvolved in the override process

Answer Area:
Answer Area

The email was [answer choice].

- sent to a manager for approval
- delivered immediately
- quarantined and undelivered
- sent to a manager for approval

The sender's manager [answer choice].

- override Rule1
- approved the email by using a workflow
- override Rule1
- was uninvolved in the override process

Section:

Explanation:

QUESTION 11

You have a Microsoft 365 tenant that has a retention label policy. You need to configure the policy to meet the following requirements:

- * Prevent the disabling or deletion of the policy.
- * Ensure that new labels can be added.
- * Prevent the removal of labels.

What should you do?

- A. Import a file plan.
- B. Enable insider risk management.
- C. Enable the regulatory record options.
- D. Create a preservation lock.

Correct Answer: D

Section:

QUESTION 12

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 are configuring a file policy in Microsoft Defender for Cloud Apps.

You need to configure the policy to apply to all files. Alerts must be sent to every file owner who is affected by the policy. The policy must scan for credit card numbers, and alerts must be sent to the Microsoft Teams site of the affected department.

Solution: You use the Built-in DIP inspection method and send alerts to Microsoft Power Automate.

Does this meet the goal?



- A. Yes
- B. No

Correct Answer: B

Section:

Explanation:

QUESTION 13

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

Name	Role	Role group
Admin1	Global Administrator	<i>None</i>
Admin2	<i>None</i>	Compliance Administrator
Admin3	<i>None</i>	Records Management

You create the retention label shown in the following exhibit.



Create retention label

Review and finish

Name
Name
Retention1
[Edit](#)

File plan descriptors

Retention settings
Retention period
7 years
[Edit](#)

Based on
Based on when it was created
[Edit](#)

Retention action
Preserve, review and delete
[Edit](#)

Disposition stages and reviewers
Stage 1 name: Stage1
Stage 1 reviewers:
Admin1@LODSe270626.onmicrosoft.com,
Admin2@LODSe270626.onmicrosoft.com,
Admin3@LODSe270626.onmicrosoft.com
[Edit](#)

Finish

Use label to classify

Which users can perform a disposition review of content that has Retention 1 applied?

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

Correct Answer: E

Section:

QUESTION 14

You have a Microsoft 365 E5 tenant that has data loss prevention (DLP) policies. You need to create a report that includes the following:

- * Documents that have a matched DLP policy.
- * Documents that have had a sensitivity label changed.

* Documents that have had a sensitivity label removed.

What should you use?

- A. an eDiscovery case
- B. communication compliance reports
- C. a content search
- D. Activity explorer

Correct Answer: C

Section:

QUESTION 15

HOTSPOT

You have a Microsoft SharePoint Online site named Site1 that contains the files shown in the following table.

Name	Number of IP addresses in the file
File1.txt	2
File2.docx	6
File3.dat	4

You have a data loss prevention (DLP) policy named DLP1 that has the advanced DIP rules shown in the following table.

Name	Content contains	Policy tip	Priority
Rule1	1 or more IP addresses	Tip1	0
Rule2	2 or more IP addresses	Tip2	1
Rule3	6 or more IP addresses	Tip3	2



You apply DLP1 to Site1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
File1.txt has the Tip1 policy tip.	<input type="radio"/>	<input type="radio"/>
File2.docx has the Tip3 policy tip.	<input type="radio"/>	<input type="radio"/>
File3.dat has the Tip2 policy tip.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
File1.txt has the Tip1 policy tip.	<input checked="" type="radio"/>	<input type="radio"/>
File2.docx has the Tip3 policy tip.	<input type="radio"/>	<input checked="" type="radio"/>
File3.dat has the Tip2 policy tip.	<input checked="" type="radio"/>	<input type="radio"/>

Section:

Explanation:

QUESTION 16

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

Correct Answer: A, C

Section:

QUESTION 17

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 compliance 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.

YOU run the Set-Mailbox -Identity 'User1' -AuditEnabled \$true command.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section:



QUESTION 18

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

Correct Answer: B

Section:

QUESTION 19

HOTSPOT

You have a Microsoft 365 subscription. In Microsoft Exchange Online, you configure the mail flow rule shown in the following exhibit.

Protect with OMEv2

 Edit rule conditions  Edit rule settings

Status: Enabled

Enable or disable rule

Enabled

Rule settings

Rule name	Mode
Protect with OMEv2	Enforce
Severity	Set date range
Not Specified	Specific date range is not set
Senders address	Priority
Matching Header	0

Rule description

Apply this rule if

*Is sent to 'Outside the organization'
and includes these words in the message subject: '[Encrypt]'*

Do the following

rights protect message with RMS template: 'Encrypt'

Rule comments



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.

Hot Area:

Answer Area

Recipients, who use Gmail, [answer choice].

- must sign in to the Office 365 Message Encryption (OME) portal to read i
- must sign in to the Office 365 Message Encryption (OME) portal to read messages
- will be unable to read messages
- will have messages decrypted automatically

Recipients from an external Microsoft 365 subscription [answer choice].

- will be unable to read messages
- must sign in to the Office 365 Message Encryption (OME) portal to read message
- will be unable to read messages
- will have messages decrypted automatically

Answer Area:

Answer Area

Recipients, who use Gmail, [answer choice].

- must sign in to the Office 365 Message Encryption (OME) portal to read i
- must sign in to the Office 365 Message Encryption (OME) portal to read messages
- will be unable to read messages
- will have messages decrypted automatically

Recipients from an external Microsoft 365 subscription [answer choice].

- will be unable to read messages
- must sign in to the Office 365 Message Encryption (OME) portal to read message
- will be unable to read messages
- will have messages decrypted automatically

Section:

Explanation:

QUESTION 20

HOTSPOT

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

Name	Type
Group1	Microsoft 365
Group2	Security

The subscription contains the resources shown in the following table.

Name	Type
Site1	Microsoft SharePoint Online site
Team1	Microsoft Teams team

You create a sensitivity label named Label 1.

You need to publish Label 1 and have the label apply automatically.

To what can you publish Label 1, and to what can Label 1 be auto-applied? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Publish to:

- Group1 and Site1 only
- Site1 only
- Group1 only
- Group1 and Group2 only
- Group1 and Site1 only**
- Site1 and Team1 only
- Group1, Group2, Site1, and Team1

Auto-apply to:

- Site1 only
- Site1 only**
- Group1 only
- Group1 and Group2 only
- Group1 and Site1 only
- Site1 and Team1 only
- Group1, Group2, Site1, and Team1

Answer Area:

Answer Area

Publish to: Group1 and Site1 only
 Site1 only
 Group1 only
 Group1 and Group2 only
Group1 and Site1 only
 Site1 and Team1 only
 Group1, Group2, Site1, and Team1

Auto-apply to: Site1 only
Site1 only
 Group1 only
 Group1 and Group2 only
 Group1 and Site1 only
 Site1 and Team1 only
 Group1, Group2, Site1, and Team1

Section:

Explanation:

QUESTION 21

HOTSPOT

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



Name	Type	Primary email address
Group1	Microsoft 365	Group1@contoso.com
Dist1	Distribution	Dist1@contoso.com

The subscription contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Dist1
User3	None

You create the mail flow rules shown in the following table.

Name	Apply this rule if	Do the following
Rule1	The recipient is a member of group1@contoso.com	Apply Office 365 Message Encryption and rights protection
Rule2	The sender is dist1@contoso.com	Apply Office 365 Message Encryption and rights protection

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
If User2 sends an email message to User3, the message is encrypted automatically.	<input type="radio"/>	<input type="radio"/>
If User2 sends an email message to User1, the message is encrypted automatically.	<input type="radio"/>	<input type="radio"/>
If User3 sends an email message to Group1, the message delivered to User1 is encrypted automatically.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
If User2 sends an email message to User3, the message is encrypted automatically.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 sends an email message to User1, the message is encrypted automatically.	<input type="radio"/>	<input checked="" type="radio"/>
If User3 sends an email message to Group1, the message delivered to User1 is encrypted automatically.	<input type="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

QUESTION 22

You need to protect documents that contain credit card numbers from being opened by users outside your company. The solution must ensure that users at your company can open the documents. What should you use?

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

Correct Answer: D

Section:

QUESTION 23

You have a Microsoft 365 E5 subscription that contains a data loss prevention (DLP) policy named DLP1. DLP1 contains the DLP rules shown in the table.

Name	Priority	User notifications	Policy tip	If there's a match for this rule, stop processing additional DLP policies and rules
Rule1	0	On	Tip 1	Enabled
Rule2	1	On	Tip 2	Enabled
Rule3	2	On	Tip 3	Disabled
Rule4	3	On	Tip 4	Enabled

You need to ensure that when a document matches all the rules, users will see Tip 2. What should you change?

- A. the priority setting of Rule2 to 0
- B. the priority setting of Rule2 to 2
- C. the priority setting of Rule3 and Rule4 to 0
- D. the If there's a match for this rule, stop processing additional DLP policies and rules setting for Rule3 to Enabled

Correct Answer: A

Section:

QUESTION 24

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 contains a file named File1.

You have a retention policy named Retention1 that has the following settings:

* Retain items for a specific period

o Retention period: 5 years o At the end of the retention period: Delete items automatically

Retention1 is applied to Site1.

You need to ensure that File1 is deleted automatically after seven years. The solution must NOT affect the retention of other files on Site1.

What should you do first?

- A. Move File1 to a new folder and list the excluded locations for Retention1.
- B. Create a new retention policy.
- C. Create and publish a new retention label
- D. Move File1 to a new folder and configure the access control list (ACL) entries for File1.

Correct Answer: C

Section:

QUESTION 25

You have a Microsoft 365 E5 subscription.

You need to identify personal data stored in the subscription and control the transfer of personal data between users and groups.

Which type of license should you acquire?

- A. Microsoft Purview Audit (Premium)
- B. Priva Privacy Risk Management
- C. Microsoft 365 E5 Compliance
- D. Priva Subject Rights Requests

Correct Answer: C

Section:

QUESTION 26

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.
You create an information barrier segment named Segment1.
You need to add Segment 1 to Site1.
What should you do first?

- A. Run the Set-SPOsite cmdlet.
- B. Run the Set-SPOTenant cmdlet.
- C. Create an information barrier policy.
- D. Modify the permissions of Site1.

Correct Answer: B

Section:

QUESTION 27

HOTSPOT

You have a Microsoft 365 E5 subscription.
You are implementing insider risk management.
You need to create an insider risk management notice template and format the message body of the notice template.
How should you configure the template? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Use the:

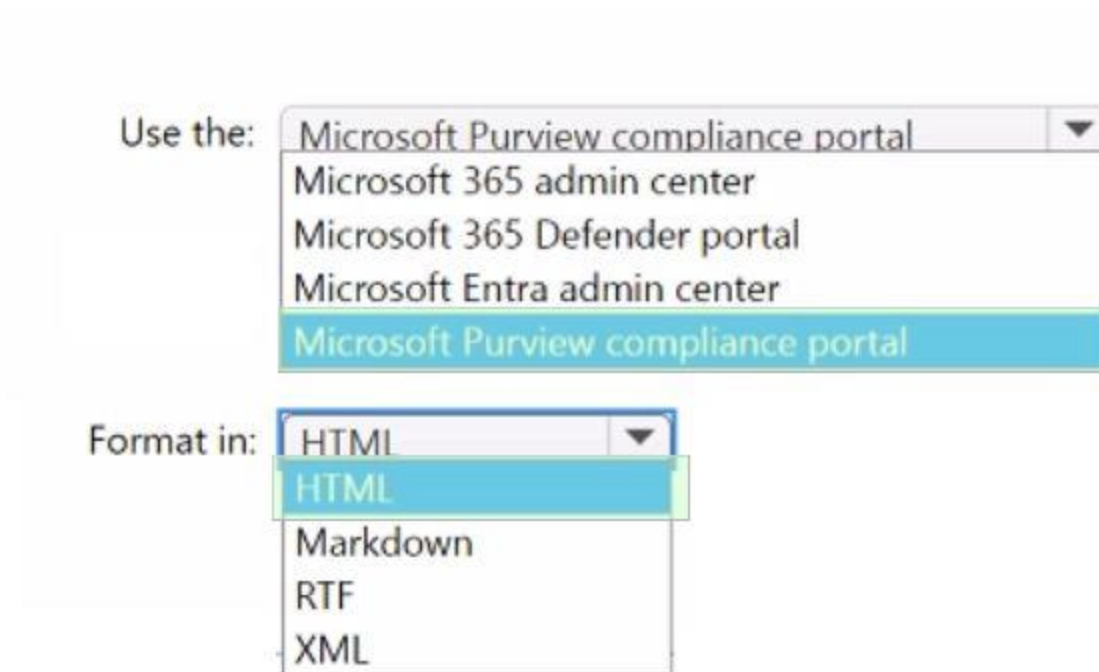
- Microsoft Purview compliance portal
- Microsoft 365 admin center
- Microsoft 365 Defender portal
- Microsoft Entra admin center
- Microsoft Purview compliance portal

Format in:

- HTML
- HTML
- Markdown
- RTF
- XML

Answer Area:

Answer Area



Section:

Explanation:

QUESTION 28

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

You need to ensure that all email messages that contain attachments are encrypted automatically by using Microsoft Purview Message Encryption.

What should you create?

- A. a sensitivity label
- B. an information barrier segment
- C. a data loss prevention (DLP) policy
- D. a mail flow rule

Correct Answer: D

Section:

QUESTION 29

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?

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

Correct Answer: D

Section:

QUESTION 30

You have a Microsoft SharePoint Online site named Site1 that contains the files shown in the following table.

Name	Number of IP addresses in the file
File1	2
File2	3

You have a data loss prevention (DLP) policy named DLP1 that has the advanced DLP rules shown in the following table.

Name	Content contains	Policy tip	If match, stop processing	Priority
Rule1	1 or more IP addresses	Tip1	No	0
Rule2	3 or more IP addresses	Tip2	Yes	1
Rule3	2 or more IP addresses	Tip3	No	2

You apply DLP1 to Site1.

Which policy tips will appear for File2?

- A. Tip1 only
- B. Tip2 only
- C. Tip3 only
- D. Tip1 and Tip2 only

Correct Answer: D

Section:

QUESTION 31

You have a Microsoft 365 E3 subscription.

You plan to audit all Microsoft Exchange Online user and admin activities.

You need to ensure that all the Exchange audit log records are retained for one year.

What should you do?

- A. Modify the record type of the default audit retention policy.
- B. Modify the retention period of the default audit retention policy.
- C. Create a custom audit retention policy.
- D. Assign Microsoft 365 Enterprise E5 licenses to all users.

Correct Answer: D

Section:

QUESTION 32

HOTSPOT

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



Name	Microsoft 365 role	Role group
Admin1	Global Administrator	None
Admin2	Compliance Administrator	None
User3	User	Compliance Manager Contributors
User4	User	Compliance Manager Administrators
User5	User	None

You create an assessment named Assesment1 as shown in the following exhibit.

Assessment1

Status **Created**
● In progress 1/15/2021

Generate report

Overview Controls Your improvement actions Microsoft actions

Review details about this assessment and understand your progress toward completion.

49% Assessment progress

1083/2169



Your points achieved ⓘ

0/1086

Microsoft managed points achieved ⓘ

1083/1083

Which users can update the title of Assesment1, and which users can add User5 to the Compliance Manager Readers role group? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Can update the Assessment1 title: ▼
User4 only
Admin2 and User4 only
Admin1, Admin2, and User4 only
Admin1, Admin2, User3, and User4 only

Can add User5 to the Compliance Manager Readers role group: ▼
Admin1 only
Admin1 and Admin2 only
Admin1 and User4 only
Admin1, Admin2, and User4 only

Answer Area:

Answer Area

Can update the Assessment1 title: ▼
User4 only
Admin2 and User4 only
Admin1, Admin2, and User4 only
Admin1, Admin2, User3, and User4 only

Can add User5 to the Compliance Manager Readers role group: ▼
Admin1 only
Admin1 and Admin2 only
Admin1 and User4 only
Admin1, Admin2, and User4 only

Section:

Explanation:

QUESTION 33

DRAG DROP

You have a Microsoft 365 E5 subscription.

You need to prevent the sharing of sensitive information in Microsoft Teams.

Which entities can you protect by applying a data loss prevention (DLP) policy to each resource? To answer, drag the appropriate activities to the correct entity. Each activity 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.

Select and Place:

Activities

- 1:1/n chats only
- Private channels only
- General chats only
- 1:1/n chats and private channels only
- 1:1/n chats and general chats only
- Private channels and general chats only
- 1:1/n chats, private channels, and general

Answer Area

User accounts:

Microsoft 365 groups:

Security groups or distribution lists:

Correct Answer:

Activities

- 1:1/n chats only
- Private channels only
-
-
-
- Private channels and general chats only
- 1:1/n chats, private channels, and general

Answer Area

User accounts: 1:1/n chats and private channels only

Microsoft 365 groups: General chats only

Security groups or distribution lists: 1:1/n chats and general chats only



Section:

Explanation:

QUESTION 34

HOTSPOT

You have a Microsoft SharePoint Online site named Site1 that contains the users shown in following table.

Name	Role
User1	Owner
User2	Member

You create the retention labels shown in the following table.

Name	Retention period	Start the retention period based on	Choose what happens after the retention period
Retention1	2 years	When items were labeled	Deactivate retention settings
Retention2	1 year	When items were labeled	Change the label to Retention1

You publish the retention labels to Site1.

Site1 contains the files shown in following table.

Name	Modified by	Retention label	Label applied
File1	User2	Retention1	August 1, 2022
File2	User1	Retention2	August 1, 2022

Which files can User1 delete on May 15,2023, and which files can User2 delete on August 15, 2024? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

May 15, 2023:

- No files
- File1 only
- File2 only
- File1 and File2

Aug 15, 2024:

- No files
- File1 only
- File2 only
- File1 and File2

Answer Area:

Answer Area

May 15, 2023:

- No files
- File1 only
- File2 only
- File1 and File2

Aug 15, 2024:

- No files
- File1 only
- File2 only
- File1 and File2



Section:

Explanation:

QUESTION 35

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

Name	Type	Query
Scope1	Users	FirstName starts with User
Scope2	SharePoint Online sites	SiteTitle starts with Site

You create the retention policies shown in the following table.

Name	Type	Location
RPolicy1	Adaptive	Scope1
RPolicy2	Adaptive	Scope2
RPolicy3	Static	Microsoft 365 groups

Which retention policies support a preservation lock?

- A. RPolicy2only
- B. RPolicy3only
- C. RPolicy1l and RPolicy2 only
- D. RPolicy1 and RPolicy3 only
- E. RPolicy1, RPolicy2, and RPolicy3

Correct Answer: D

Section:

QUESTION 36

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 compliance 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.

YOU run the Set-AdminAuditLogConfig -AdminAuditLogEnabled \$true -AdminiAuditLogCmdlets 'Mailbox*' command.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

QUESTION 37

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 compliance 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.

YOU run the Set-MailboxFolderPernission -Identity 'User1' -User User1fcontoso.com -AccessRights Owner command.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

QUESTION 38

You have a Microsoft 365 E5 subscription.
You are implementing insider risk management.
You need to maximize the amount of historical data that is collected when an event is triggered.
What is the maximum number of days that historical data can be collected?

- A. 30
- B. 60
- C. 90
- D. 180

Correct Answer: C

Section:

QUESTION 39

You have a Microsoft 365 E5 subscription that uses Microsoft Purview. The subscription contains two groups named Group1 and Group2.
You need to implement a policy to detect messages that present a conflict of interest between the users in Group1 and the users in Group2.
What should you use in the Microsoft Purview compliance portal?

- A. Insider risk management
- B. Privacy risk management
- C. Information barriers
- D. Communication compliance

Correct Answer: D

Section:



QUESTION 40

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 E5 subscription.

You need to identify resumes that are stored in the subscription by using a built-in trainable classifier.

Solution: You create an auto-labeling policy for a sensitivity label.

Does this meet the goal?

- A. Yes
- B. NO

Correct Answer: A

Section:

QUESTION 41

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 E5 subscription.

You need to identify resumes that are stored in the subscription by using a built-in trainable classifier.

Solution: You create a data loss prevention (DLP) policy.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B
Section:

QUESTION 42

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

Name	Role group
Admin1	eDiscovery Manager
Admin2	eDiscovery Administrator
Admin3	<i>none</i>

You need to ensure that Admin3 can create holds in owing table.
To what should you add Admin3?

- A. the Global Administrator role
- B. the eDiscovery Manager role group
- C. the Compliance Manager Contributors role group
- D. the eDiscovery Administrator role group

Correct Answer: B
Section:

QUESTION 43

HOTSPOT

You have a Microsoft 365 E5 subscription.

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

- * Prevents users from performing data transfers that breach local regulations
- * Minimizes effort to respond to requests for a user's personal data

What should you use in the Microsoft Purview compliance portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

To prevent users from performing data transfers that breach local regulations:

- Information barriers
- Communication compliance
- Information barriers
- Insider risk management
- Privacy risk management

To minimize effort to respond to requests for a user's personal data:

- Subject rights request
- Data loss prevention (DLP)
- eDiscovery
- Records management
- Subject rights request

Answer Area:

Answer Area

To prevent users from performing data transfers that breach local regulations:

- Information barriers
- Communication compliance
- Information barriers
- Insider risk management
- Privacy risk management

To minimize effort to respond to requests for a user's personal data:

- Subject rights request
- Data loss prevention (DLP)
- eDiscovery
- Records management
- Subject rights request

Section:

Explanation:

QUESTION 44

You have a Microsoft 365 E5 subscription that uses Microsoft Teams and contains a user named User1. You configure Microsoft Purview Information Barriers. You need to identify which information barrier policies apply to User1. Which cmdlet should you use?

- A. Get-OrganizationSeagent
- B. Get-InformationBarrierPoliciesApplicationStatus
- C. Get-InformationBarrierPolicy
- D. Get-InformationBarrierRecipientStatus

Correct Answer: D

Section:

QUESTION 45

You have a Microsoft 365 E5 subscription. You need to create a subject rights request. What can be configured as a search location?

- A. Microsoft Exchange Online and Teams only
- B. Microsoft Exchange Online, SharePoint Online, and Teams
- C. Microsoft Exchange Online only
- D. Microsoft Exchange Online and SharePoint Online only
- E. Microsoft SharePoint Online only

Correct Answer: B

Section:

QUESTION 46

You have a Microsoft 365 E5 subscription.

You need to prevent users from uploading data loss prevention (DLP)-protected documents to the following third-party websites;

* web1.contoso.com

* web2.contoso.com

The solution must minimize administrative effort.

To what should you set the Service domains setting for Endpoint DLP?

- A. contoso.com
- B. web'.contoso.com
- C. *.contoso.com
- D. web1xontoso.com and web2.contoso.com



Correct Answer: D

Section:

QUESTION 47

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 compliance 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

Correct Answer: B

Section:

QUESTION 48

You have a Microsoft 365 E5 tenant that contains a Microsoft SharePoint Online document library named Library 1. You need to declare a collection of files that are stored in Library1 as regulatory records. What should you use?

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

Correct Answer: D

Section:

QUESTION 49

You have a Microsoft 365 E5 subscription. You plan to implement retention policies for Microsoft Teams. Which item types can be retained?

- A. voice memos from the Teams mobile client
- B. embedded images
- C. code snippets

Correct Answer: A

Section:

QUESTION 50

You have a Microsoft 365 E5 subscription. You need to export the details of a retention label. The export must include the following information;
* Is record
* Is regulatory
* Disposition type
What should you do?

- A. From the Microsoft Purview compliance portal, export Compliance Manager assessment actions.
- B. From the Microsoft Purview compliance portal export a file plan.
- C. From the Microsoft Purview compliance portal export a disposition review.
- D. From PowerShell, run the Export-ActivityExplorerData cmdlet.
- E. From PowerShell, run the Get-RetentionEvent cmdlet.

Correct Answer: B

Section:

QUESTION 51

You have a Microsoft 365 E5 subscription that uses Yammer. You need to create a Microsoft Purview communication compliance policy that will detect inappropriate images in Yammer conversations. What should you do first?

- A. Configure Hybrid Mode for Yammer.



- B. Configure the Yammer network admin settings.
- C. Assign each user a Yammer license.
- D. Configure Native Mode for Yammer.

Correct Answer: C

Section:

QUESTION 52

You create a label that encrypts email data.

Users report that they cannot use the label in Outlook on the web to protect the email messages they send.

You need to ensure that the users can use the new label to protect their email.

What should you do?

- A. Wait six hours and ask the users to try again.
- B. Create a label policy.
- C. Create a new sensitive information type.
- D. Modify the priority order of label policies

Correct Answer: D

Section:

QUESTION 53

You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group 1 contains 100 users and has dynamic user membership.

All users have Windows 10 devices and use Microsoft SharePoint Online and Exchange Online.

You create a sensitivity label named Label1 and publish Label1 as the default label for Group1.

You need to ensure that the users in Group1 must apply Label1 to their email and documents.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. From the Microsoft Purview compliance portal, modify the settings of the Label1 policy.
- B. From the Azure Active Directory admin center, set Membership type for Group1 to Assigned.
- C. Install the Azure Information Protection unified labeling client on the Windows 10 devices.
- D. Install the Active Directory Rights Management Services (AD RMS) client on the Windows 10 devices.
- E. From the Microsoft Purview compliance portal, create an auto-labeling policy.

Correct Answer: A, C

Section:

QUESTION 54

HOTSPOT

You have a Microsoft 365 sensitivity label that is published to all the users in your Azure AD tenant as shown in the following exhibit.

Hot Area:

Answer Area

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

Answer Area:
Answer Area

Statements	Yes	No
All the documents stored on each user's computer will include a watermark automatically.	<input type="radio"/>	<input checked="" type="radio"/>
If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL".	<input type="radio"/>	<input checked="" type="radio"/>
The sensitivity label can be applied only to documents that contain the word rebranding.	<input type="radio"/>	<input checked="" type="radio"/>

Section:
Explanation:

QUESTION 55

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 OC.
- C. a function
- D. an exact data match (EDM) classifier

Correct Answer: A

Section:

QUESTION 56

You have a Microsoft 365 subscription.

You create and run a content search from the Microsoft Purview compliance portal.

You need to download the results of the content search.

What should you obtain first?

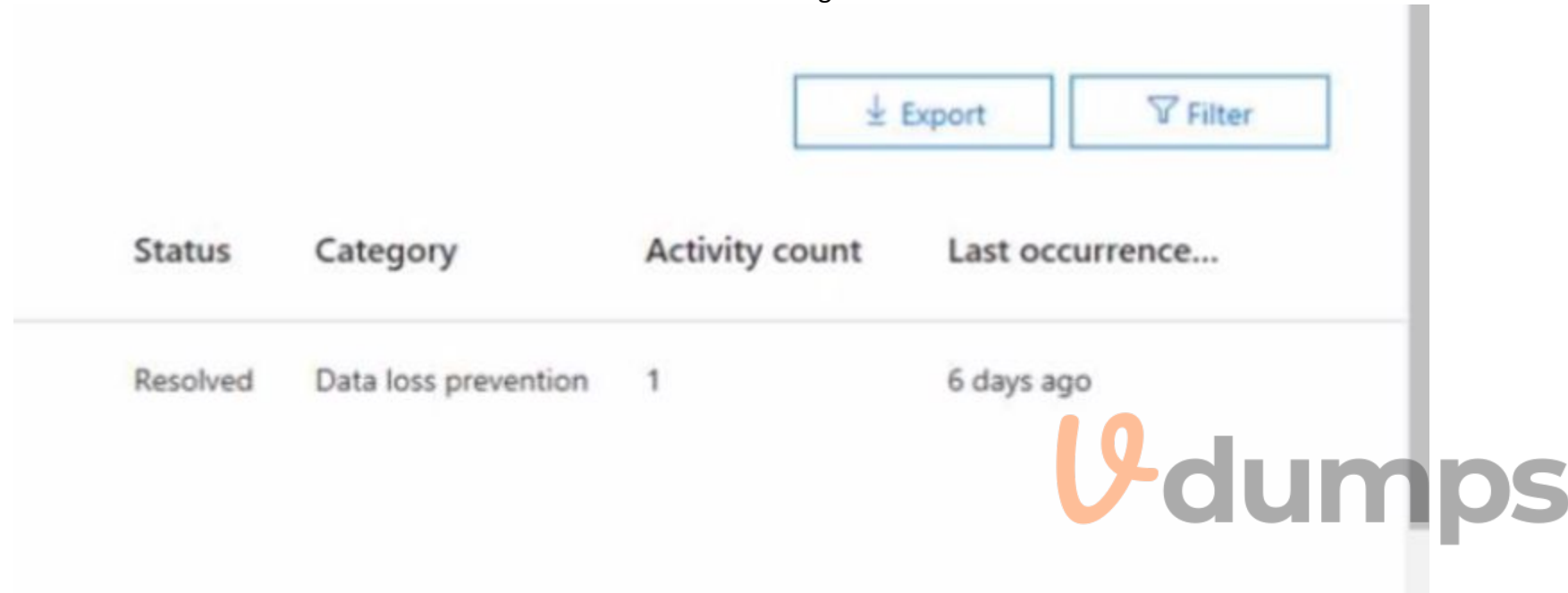
- A. a certificate
- B. a password
- C. a pin
- D. an export key

Correct Answer: D

Section:

QUESTION 57

You have a Microsoft 365 alert named Alert2 as shown in the following exhibit



Status	Category	Activity count	Last occurrence...
Resolved	Data loss prevention	1	6 days ago

You need to manage the status of Alert2. To which status can you change Alert2?

- A. The status cannot be changed.
- B. Dismissed only
- C. Investigating only
- D. Active or Investigating only
- E. Investigating, Active, or Dismissed

Correct Answer: E

Section:

QUESTION 58

HOTSPOT

You have a Microsoft 365 subscription. Auditing is enabled.

A user named User1 is a member of a dynamic security group named Group1.

You discover that User1 is no longer a member of Group1.

You need to search the audit log to identify why User1 was removed from Group1.

Which two activities should you use in the search? To answer, select the appropriate activities in the answer area.

Hot Area:

Answer Area

Search

Clear

Results

Activities

Date ▼

IP address

User

Activity

Item

Show results for all activities

x Clear all to show results for all activities

Search

User administration activities

Added user

Deleted user

Set license properties

Reset user password

Changed user password

Changed user license

Updated user

Set property that forces user to change password

Azure AD group administration activities

Added group

Updated group

Deleted group

Added member to group

Removed member from group

Application administration activities

Added service principal

Removed a service principal from the directory

Set delegation entry

Removed credentials from a service principal

Added delegation entity

Added credentials to a service principal

Answer Area:

Answer Area

Search

Clear

Results

Activities

Date ▼

IP address

User

Activity

Item

Show results for all activities

x Clear all to show results for all activities

Search

User administration activities

Added user

Deleted user

Set license properties

Reset user password

Changed user password

Changed user license

Updated user

Set property that forces user to change password

Azure AD group administration activities

Added group

Updated group

Deleted group

Added member to group

Removed member from group

Application administration activities

Added service principal

Removed a service principal from the directory

Set delegation entry

Removed credentials from a service principal

Added delegation entity

Added credentials to a service principal

Section:

Explanation:

QUESTION 59

You have a Microsoft 365 subscription.

You have a team named Team1 in Microsoft Teams.

You plan to place all the content in Team1 on hold.

You need to identify which mailbox and which Microsoft SharePoint site collection are associated to Team1.

Which cmdlet should you use?

- A. Get-UnifiedGroup
- B. Get-MalUser
- C. Get-TeamChannel
- D. Get-Team

Correct Answer: D

Section:

QUESTION 60

You have a Microsoft 365 subscription.

You need to be notified by email whenever an administrator starts an eDiscovery search.

What should you do from the Microsoft Purview compliance portal?

- A. From eDiscovery, create an eDiscovery case.
- B. From Policies, create an alert policy.
- C. From Records management, create event type.
- D. From Content search, create a new search.

Correct Answer: B

Section:

QUESTION 61

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

You need to assign User1 permissions to search Microsoft Office 365 audit logs.

What should you use?

- A. the Azure Active Directory admin center
- B. the Microsoft Purview compliance portal
- C. the Exchange admin center
- D. the Microsoft 365 Defender portal

Correct Answer: C

Section:

QUESTION 62

You have a Microsoft 365 E5 subscription that contains two Microsoft SharePoint Online sites named Site1 and Site2.

You plan to configure a retention label named Label1 and apply Label1 to all the files in Site1.

You need to ensure that two years after a file is created in Site1, the file moves automatically to Site2.

How should you configure the Choose what happens after the retention period setting for Label1?

- A. Run a Power Automate flow
- B. Change the label
- C. Deactivate retention settings
- D. Start a disposition review



Correct Answer: A

Section:

QUESTION 63

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.

Select and Place:

Filters	Answer Area
Access level	When a file is shared externally. <input type="text"/>
Collaborators	When a file is labelled as Internal only. <input type="text"/>
Matched policy	
Sensitivity label	



Correct Answer:

Filters	Answer Area
<input type="text"/>	When a file is shared externally. <input type="text" value="Access level"/>
Collaborators	When a file is labelled as Internal only. <input type="text" value="Sensitivity label"/>
Matched policy	
<input type="text"/>	

Section:

Explanation:

QUESTION 64

HOTSPOT

You have a Microsoft 36d tenant.

You need to create a new sensitive info type for items that contain the following:

* An employee ID number that consists of the hire date of the employee followed by a three-digit number

* The words 'Employee', 'ID', or 'Identification' within 300 characters of the employee ID number
What should you use for the primary and secondary elements? To answer, select the appropriate options in the answer area.

Hot Area:

Answer Area

Primary element:

Secondary element:

Answer Area:

Answer Area

Primary element:

Secondary element:

Section:

Explanation:

QUESTION 65

HOTSPOT

You have a Microsoft 365 tenant.

You need to create a new sensitive info type for items that contain the following:

- * An employee ID number that consists of the hire date of the employee followed by a three-digit number
- * The words 'Employee', 'ID', or 'Identification' within 300 characters of the employee ID number

What should you use for the primary and secondary elements? To answer, select the appropriate options in the answer area.

Hot Area:

Answer Area

Primary element:

Secondary element:

Answer Area:

Answer Area

Primary element:

Secondary element:

Section:

Explanation:

QUESTION 66

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

Name	Type	Location
Mail1	Email message	Microsoft Exchange Online
File1.docx	File	Microsoft SharePoint Online
File2.xlsx	File	Microsoft OneDrive

You have a retention label configured as shown in the following exhibit.

Define retention settings

When this label is applied to items, the content is retained and/or deleted based on the settings you choose here.

Retain items for a specific period

Labeled items will be retained for the period you choose.

Retention period

Start the retention period based on

+ Create new event type

During the retention period

Retain items even if users delete

Users will be able to edit items and change or remove the label. If they delete items, we'll keep copies in a secure location. [Learn more](#)

Mark items as a record

At the end of the retention period

Delete items automatically

We'll delete items from where they're currently stored.

Trigger a disposition review

Do nothing

Items will be left in place. You'll have to manually delete them if you want them gone.



You publish the retention label and set the scope as shown in the following exhibit.

Choose locations

We'll publish the labels to the locations you choose.

All locations. Includes content in Exchange email, Office 365 groups, OneDrive and SharePoint documents.

Let me choose specific locations.

You apply the label to the resources.

Which items can you delete?

Choose the correct answer:

- A Mail1 only
- B File1.docx and File2.xlsx only
- C Mail1 and File1.docx only
- D Mail1 and File2.xlsx only
- E Mail1, File1.docx, and File2.xlsx

A.

Correct Answer:

Section:

QUESTION 67

You have a Microsoft 365 E5 subscription that uses Privacy Risk Management in Microsoft Priva.

You need to review the personal data type instances that were detected in the subscription.

What should you use in the Microsoft Purview compliance portal?

- A. Content explorer
- B. User data search
- C. Content search
- D. an eDiscovery case

Correct Answer: A

Section:



QUESTION 68

DRAG DROP

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

You need to implement insider risk management. The solution must meet the following requirements:

- * Ensure that User1 can create insider risk management policies.
- * Ensure that User2 can use content captured by using insider risk management policies.
- * Follow the principle of least privilege.

To which role group should you add each user? To answer, drag the appropriate role groups to the correct users. Each role group 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.

Select and Place:

Role groups

-
-
-
-
-

Answer AreaUser1: User2: **Correct Answer:****Role groups**

-
-
-
-
-

Answer AreaUser1: User2: **Section:****Explanation:****QUESTION 69**

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

Name	Department
User1	Finance
User2	Research
User3	Finance

You need to prevent users in the finance department from sharing files with users in the research department. Which type of policy should you configure?

- A. communication compliance
- B. information barrier
- C. Conditional Access
- D. insider risk management

Correct Answer: B**Section:**

QUESTION 70

HOTSPOT

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

Name	Type	User principal name (UPN)	Member of
User1	User	user1@sk220115outlook.onmicrosoft.com	Dist1
User2	User	user2@sk220115outlook.onmicrosoft.com	Dist1
User3	User	user3@sk220115outlook.onmicrosoft.com	Group1
User4	User	user4@sk220115outlook.onmicrosoft.com	none
Group1	Microsoft 365 group	group1@sk220115outlook.onmicrosoft.com	none
Dist1	Distribution group	dist1@sk220115outlook.onmicrosoft.com	none

You create the communication compliance policy as shown in the exhibit. (Click the Exhibit tab.)



Review and finish

Name and description

Name

CommCompliance1

Users and reviewers

Supervised users and groups

dist1@sk220115outlook.onmicrosoft.com,Group1@sk220115outlook.onmicrosoft.com

Excluded users and groups

User2@sk220115outlook.onmicrosoft.com

Reviewers

User4@sk220115outlook.onmicrosoft.com

Locations

Monitored locations

Exchange

Conditions and percentage

Communication direction

Inbound

Optical character recognition(OCR)

Disabled

Conditions

None

Percentage to review

100



Four emails are sent as shown in the following table.

Name	Description
Mail1	Sent by User3 to User1.
Mail2	Sent by User1 to User2.
Mail3	Sent by User2 to User1.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
 NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User4 can review Mail1.	<input type="radio"/>	<input type="radio"/>
User4 can review Mail2.	<input type="radio"/>	<input type="radio"/>
User4 can review Mail3.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area



Statements	Yes	No
User4 can review Mail1.	<input type="radio"/>	<input checked="" type="radio"/>
User4 can review Mail2.	<input type="radio"/>	<input checked="" type="radio"/>
User4 can review Mail3.	<input type="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

QUESTION 71

HOTSPOT

You have a hybrid Microsoft 365 deployment that contains the users shown in the following table.

Name	Mailbox	Cloud license
User1	On-premises Microsoft Exchange Server	Microsoft Teams
User2	On-premises Microsoft Exchange Server	Microsoft Exchange Online Plan 2
User3	On-premises Microsoft Exchange Server	Microsoft Teams, Exchange Online Plan 2
User4	Microsoft Exchange Online	Microsoft Teams, Exchange Online Plan 2

You need to perform an eDiscovery content search.

Which user's data can be included in the content search? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Exchange mailboxes:

- User4 only
- User4 and User3 only**
- User4, User3, and User2 only
- User4, User3, User2, and User1

Teams chat data:

- User4 only
- User4 and User3 only
- User4, User3, and User1 only**
- User4, User3, User2, and User1

Answer Area:

Answer Area

Exchange mailboxes:

- User4 only
- User4 and User3 only**
- User4, User3, and User2 only
- User4, User3, User2, and User1

Teams chat data:

- User4 only
- User4 and User3 only
- User4, User3, and User1 only**
- User4, User3, User2, and User1

Section:

Explanation:

QUESTION 72**HOTSPOT**

You have a Microsoft 365 subscription that has Enable Security defaults set to No in Azure AD.

You have a custom compliance manager template named Regulation1.

You have the assessments shown in the following table.

Name	Score	Status	Group	Product	Regulation
Assessment1	1200	Incomplete	Group1	Microsoft 365	Regulation1
Assessment2	900	Incomplete	Group2	Microsoft 365	Regulation1

Assessment1 has the improvement actions shown in the following table.

Improvement action	Test status	Impact	Points achieved	Action type
Enable multi-factor authentication for admins	Failed high risk	+27 points	0/27	Technical
Enable multi-factor authentication for non-admins	Failed high risk	+27 points	0/27	Technical

Assessment2 has the improvement actions shown in the following table.

Improvement action	Test status	Impact	Points achieved	Action type
Establish a threat intelligence program	None	+9 points	0/9	Operational
Configure a privileged access policy	Failed high risk	+15 points	0/15	Technical

You perform the following actions:

* For Assessment2, change the Test status of Establish a threat intelligence program to Implemented.

* Enable multi-factor authentication (MFA) for all users.

* Configure a privileged access policy.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in Assessment1.	<input type="radio"/>	<input type="radio"/>
The Assessment1 score will increase by only 54 points.	<input type="radio"/>	<input type="radio"/>
The Assessment2 score will increase by only 78 points.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in Assessment1.	<input checked="" type="radio"/>	<input type="radio"/>
The Assessment1 score will increase by only 54 points.	<input checked="" type="radio"/>	<input type="radio"/>
The Assessment2 score will increase by only 78 points.	<input checked="" type="radio"/>	<input type="radio"/>

Section:

Explanation:

QUESTION 73

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

Name	Type	Location
Mail1	Email message	Microsoft Exchange Online
File1.docx	File	Microsoft SharePoint Online
File2.xlsx	File	Microsoft OneDrive

You have a retention label configured as shown in the following exhibit.



Define retention settings

When this label is applied to items, the content is retained and/or deleted based on the settings you choose here.

Retain items for a specific period

Labeled items will be retained for the period you choose.

Retention period

Start the retention period based on

+ Create new event type

During the retention period

Retain items even if users delete

Users will be able to edit items and change or remove the label. If they delete items, we'll keep copies in a secure location. [Learn more](#)

Mark items as a record

At the end of the retention period

Delete items automatically

We'll delete items from where they're currently stored.

Trigger a disposition review

Do nothing

Items will be left in place. You'll have to manually delete them if you want them gone.



You publish the retention label and set the scope as shown in the following exhibit.

Choose locations

We'll publish the labels to the locations you choose.

All locations. Includes content in Exchange email, Office 365 groups, OneDrive and SharePoint documents.

Let me choose specific locations.

You apply the label to the resources.
Which items can you delete?

- A. Mail1 only
- B. File1.docx and File2.xlsx only
- C. Mail1 and File1.docx only
- D. Mail1 and File2.xlsx only
- E. Mail1, File1.docx, and File2.xlsx

Correct Answer: E
Section:

QUESTION 74

You have a Microsoft 365 tenant that has data loss prevention (DLP) policies.
You need to review DLP policy matches for the tenant.
What should you use?

- A. Content explorer
- B. Activity explorer
- C. Compliance Manager
- D. records management events

Correct Answer: B
Section:



QUESTION 75

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.
On January 1, you create the sensitivity label shown in the following table.

Setting	Value
Name	Label1
Assign permissions now or let users decide?	Assign permissions now
User access to content expires	After 21 days
Assign permissions to specific users and groups	Co-Author: User1 and User2

On January 2, you publish Label1 to User1.
On January 3, User1 creates a Microsoft Word document named Doc1 and applies Label1 to the document.
On January 4, User2 edits Doc1.
On January 15, you increase the content expiry period for Label1 to 28 days.
When will access to Doc1 expire for User2?

- A. January 23
- B. January 24
- C. January 25
- D. January 31

Correct Answer: C

Section:

QUESTION 76

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 10. 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

Correct Answer: B

Section:

QUESTION 77

HOTSPOT

You have a Microsoft 365 subscription.

You are creating a retention policy named Retention1 as shown in the exhibit. (Click the Exhibit tab.)



Decide if you want to retain content, delete it, or both

Retain items for a specific period
Items will be retained for the period you choose.

Retain items for a specific period

of years months days

Start the retention period based on

At the end of the retention period

Delete items automatically

Do nothing

Retain items forever
Items will be retained forever, even if users delete them.

Only delete items when they reach a certain age
Items won't be retained, but when they reach the age you choose, we'll delete them from where they're stored.



You apply Retention1 to SharePoint sites and OneDrive accounts.
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.

Hot Area:

Answer Area

If a user creates a file in a Microsoft SharePoint library on January 1, 2023, and modifies the file every six months, the file will be **[answer choice]**.

If a user creates a file in Microsoft OneDrive on January 1, 2023, modifies the file on March 1, 2023, and deletes the file on May 1, 2023, the user **[answer choice]**.

Answer Area:

Answer Area

If a user creates a file in a Microsoft SharePoint library on January 1, 2023, and modifies the file every six months, the file will be **[answer choice]**.

- retained
- retained**
- deleted on January 1, 2025
- deleted on July 1, 2025

If a user creates a file in Microsoft OneDrive on January 1, 2023, modifies the file on March 1, 2023, and deletes the file on May 1, 2023, the user **[answer choice]**.

- can recover the file until March 1, 2025
- can recover the file until the Recycle Bin retention period expires
- can recover the file until January 1, 2025
- can recover the file until March 1, 2025**
- can recover the file until May 1, 2025

Section:

Explanation:

QUESTION 78

HOTSPOT

You have a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com.

OneDrive stores files that are shared with external users. The files are configured as shown in the following table.

Name	Applied label
File1	Label1
File2	Label1, Label2
File3	Label2



You create a data loss prevention (DLP) policy that applies to the content stored in OneDrive accounts. The policy contains the following three rules:

Rule1:

- * Conditions: Label1. Detect content that's shared with people outside my organization
- * Actions: Restrict access to the content for external users
- * User notifications: Notify the user who last modified the content
- * User overrides: On
- * Priority: 0

Rule2:

- * Conditions: Label1 or Label2
- * Actions: Restrict access to the content
- * Priority: 1

Rule3:

- * Conditions: Label2. Detect content that's shared with people outside my organization
- * Actions: Restrict access to the content for external users
- * User notifications: Notify the user who last modified the content
- * User overrides: On
- * Priority: 2

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
External users can access File1.	<input type="radio"/>	<input type="radio"/>
The users in contoso.com can access File2.	<input type="radio"/>	<input type="radio"/>
External users can access File3.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
External users can access File1.	<input type="radio"/>	<input checked="" type="checkbox"/>
The users in contoso.com can access File2.	<input type="radio"/>	<input checked="" type="checkbox"/>
External users can access File3.	<input type="radio"/>	<input checked="" type="checkbox"/>

Section:

Explanation:

QUESTION 79

You plan to create a new data loss prevention (DLP) policy named DLP1. DLP1 will be applied to the Exchange email location. You need to exclude two users named User1 and User2 from DLP1. What should you do first?

- A. Create an organization sharing policy in Microsoft Exchange.
- B. Create a mail flow rule in Microsoft Exchange.
- C. Create a distribution list that contains User1 and User2.
- D. Create an advanced DLP rule.

Correct Answer: C

Section:

QUESTION 80

HOTSPOT

You have a Microsoft 365 E5 subscription that contains two users named Admin1 and User1, a Microsoft SharePoint Online site named Site1, and a retention label named Retention1. The role assignments for Site1 are shown in the following table.



Name	Role
Admin1	Owner
User1	Member

Site1 includes a file named File1. Retention1 has the following settings:

- * Retain items for a specific period: Retention period: 7 years
- * During the retention period: Mark items as a record
- * At the end of the retention period: Delete items automatically

Retention1 is published to Site1. User1 applies Retention1 to File1. For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can rename File1.	<input type="radio"/>	<input type="radio"/>
Admin1 can modify the contents of File1.	<input type="radio"/>	<input type="radio"/>
User1 can remove Retention1 from File1.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
User1 can rename File1.	<input checked="" type="radio"/>	<input type="radio"/>
Admin1 can modify the contents of File1.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can remove Retention1 from File1.	<input type="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

QUESTION 81

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-SPOService
- B. Connect-IPPSSession

- C. Connect-AzureAD
- D. Connect-ExchangeOnline

Correct Answer: C

Section:

QUESTION 82

HOTSPOT

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the groups shown in the following table.

Name	Type	Email address
Group1	Security Group – Domain Local	Group1@contoso.com
Group2	Security Group - Universal	None
Group3	Distribution Group - Global	None
Group4	Distribution Group - Universal	Group4@contoso.com

The domain is synced to an Azure AD tenant that contains the groups shown in the following table.

Name	Type	Membership type
Group11	Security group	Assigned
Group12	Security group	Dynamic
Group13	Microsoft 365 group	Assigned
Group14	Mail-enabled security group	Assigned

You create a sensitivity label named Label1.

You need to publish Label1.

To which groups can you publish Label1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

On-premises Active Directory groups:

- Group1 and Group4 only
- Group4 only
- Group1 and Group4 only**
- Group3 and Group4 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Azure AD groups:

- Group13 and Group14 only
- Group13 only
- Group13 and Group14 only**
- Group 11 and Group 12 only
- Group11, Group13, and Group14 only
- Group11, Group12, Group13, and Group14

Answer Area:

Answer Area

On-premises Active Directory groups:

- Group1 and Group4 only
- Group4 only
- Group1 and Group4 only**
- Group3 and Group4 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Azure AD groups:

- Group13 and Group14 only
- Group13 only
- Group13 and Group14 only**
- Group 11 and Group 12 only
- Group11, Group13, and Group14 only
- Group11, Group12, Group13, and Group14

Section:

Explanation:

QUESTION 83

HOTSPOT

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

Name	Role
User1	Information Protection Administrator
User2	Information Protection Analyst
User3	Information Protection Investigator



You need to delegate the following tasks:

- * Create and manage data loss prevention (DLP) policies.
- * Review classified content by using Content explorer.

The solution must use the principle of least privilege.

Which user should perform each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Create and manage DLP policies:

- User1
- User1**
- User2
- User3

Review classified content by using Content explorer:

- User3
- User1
- User2
- User3**

Answer Area:

Answer Area

Create and manage DLP policies:

User1
User1
User2
User3

Review classified content by using Content explorer:

User3
User1
User2
User3

Section:

Explanation:

QUESTION 84

HOTSPOT

You have a Microsoft 365 subscription.

You need to use PowerShell to enable multiple segment support for information barriers (IBs).

How should you complete the PowerShell command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Set-PolicyConfig
New-OrganizationSegment
Set-InformationBarrierPolicy
Set-PolicyConfig

-InformationBarrierMode
-InformationBarrierMode
-InformationBarrierPeopleSearchRestriction
-UserGroupFilter

'MultiSegment'

Answer Area:

Answer Area

Set-PolicyConfig
New-OrganizationSegment
Set-InformationBarrierPolicy
Set-PolicyConfig

-InformationBarrierMode
-InformationBarrierMode
-InformationBarrierPeopleSearchRestriction
-UserGroupFilter

'MultiSegment'

Section:

Explanation:

QUESTION 85

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 Entra admin center, create a security group.
- B. From the Microsoft Purview compliance portal, create a priority user group.
- C. From the Microsoft Entra admin center, create a User risk policy.

D. From the Microsoft Purview compliance portal, create an insider risk management policy.

Correct Answer: B

Section:

QUESTION 86

DRAG DROP

You have a Microsoft 365 E5 subscription

You need to configure the Microsoft Priva Privacy Risk Management policies to generate alerts for the following scenarios:

* Scenario1: A user shares a Microsoft SharePoint Online document library link with a user in a different country.

* Scenario2: A user from the sales department emails personal data to a user in a different country.

* Scenario3: The personal data stored on a Microsoft SharePoint Online site was NOT modified during the last 120 days.

Which policy template should you use for each scenario? To answer, drag the appropriate policy templates to the correct scenarios. Each template 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.

Select and Place:

Policy templates

- ☰ Data minimization
- ☰ Data overexposure
- ☰ Data transfers

Answer Area



Correct Answer:

Policy templates

-
-
-

Answer Area



Scenario1:

Scenario2:

Scenario3:



Scenario1: ☰ Data minimization

Scenario2: ☰ Data transfers

Scenario3: ☰ Data overexposure

Section:

Explanation:

QUESTION 87

DRAG DROP

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

You need to create a custom sensitive info type. The solution must meet the following requirements:

* Match product serial numbers that contain a 10-character alphanumeric string.

* Ensure that the abbreviation of SN appears within six characters of each product serial number.

* Exclude a test serial number of 1111111111 from a match.

Which pattern settings should you configure for each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting 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.

Select and Place:

Settings

- Additional checks
- Character proximity
- Confidence level
- Primary element
- Supporting elements

Answer Area

Match product serial numbers that contain a 10-character alphanumeric string:

Ensure that the abbreviation of SN appears within six characters of each product serial number:

Exclude a test serial number of 1111111111 from a match:

Correct Answer:

Settings

- Confidence level
- Supporting elements

Answer Area

Match product serial numbers that contain a 10-character alphanumeric string:

Ensure that the abbreviation of SN appears within six characters of each product serial number:

Exclude a test serial number of 1111111111 from a match:



Section:

Explanation:

QUESTION 88

HOTSPOT

You have a Microsoft 365 E5 tenant that contains a published sensitivity label named Sensitivity1. You plan to create a Microsoft Entra group named Group1 and assign Sensitivity1 to Group1. How should you configure Group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

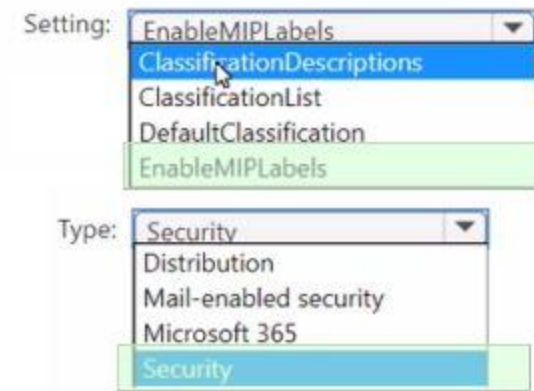
Answer Area

Setting:

Type:

Answer Area:

Answer Area



Section:

Explanation:

QUESTION 89

You have a Microsoft 365 E3 subscription.

You plan to assess compliance with ISO/IEC 27001:2013.

From Compliance Manager, you discover that the ISO/IEC 27001:2013 regulatory template for Microsoft 365 is inactive.

What should you do?

- A. Add recommended assessments.
- B. Add a data connector.
- C. Create a trainable classifier.
- D. Purchase a Microsoft 365 E5 subscription.

Correct Answer: D

Section:

