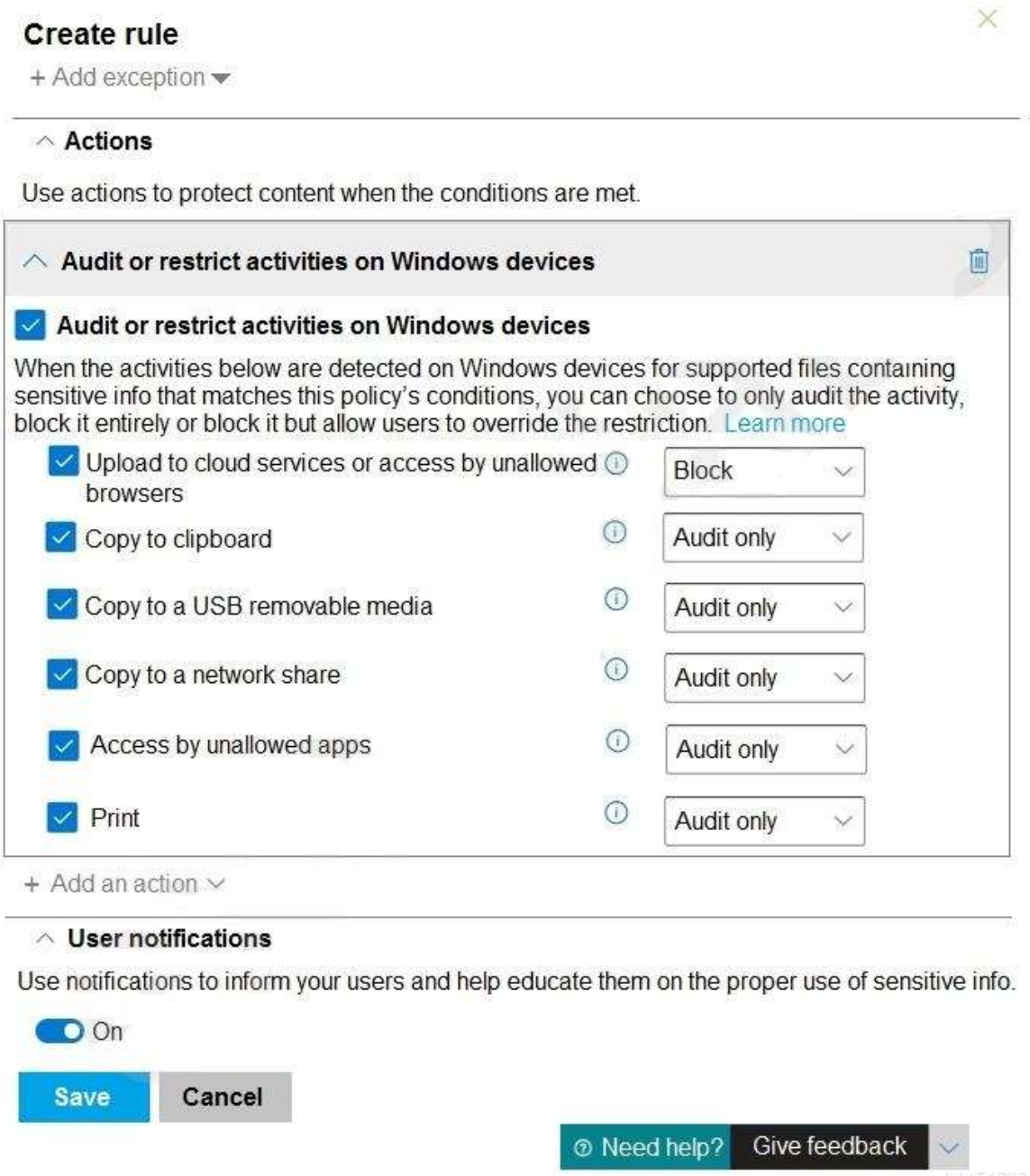
QUESTION 87
You are planning a data loss prevention (DLP) solution that will apply to computers that run Windows 10.
You need to ensure that when users attempt to copy a file that contains sensitive information to a USB storage device, the following requirements are met:
- If the users are members of 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. one DLP policy that contains one DLP rule
B. two DLP policies that each contains on DLP rule
C. one DLP policy that contains two DLP rules

Answer: B

QUESTION 88
You have a data loss prevention (DLP) policy configured for endpoints as shown in the following exhibit.



From a computer named Computer1, 3 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 Access by unallowed apps action is set to Audit only.
B. The computers are NOT onboarded to the Microsoft 365 compliance center.
C. The Copy to clipboard action is set to Audit only.
D. There are file path exclusions in the Microsoft 365 Endpoint data loss prevention (Endpoint DIP) settings.
E. The unallowed browsers in the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings are NOT configured.

Answer: AD

QUESTION 89
You need to be alerted when users share sensitive documents from Microsoft OneDrive to any users outside your company.
What should you do?

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

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

QUESTION 90
Your company manufactures parts that are each assigned a unique 12-character alphanumeric serial number. Emails between the company and its customers refer in the serial number.
You need to ensure that ail 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 trainable classifier
B. a sensitive info type
C. a retention polity
D. a data loss prevention (DLP) policy
E. an auto-labeling policy
F. a retention label
G. a sensitivity label

Answer: BEF
Explanation:
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 91
You receive an email that contains a list of words that will be used few a sensitive information type.
You need to create a file that can be used as the source of a keyword dictionary.
In which format should you save the list?

A. an XLSX file that contains one word in each cell of the first row
B. a ISV file that contains words separated by tabs
C. a JSON file that that an element tor each word
D. a text file that has one word on each line

Answer: A

QUESTION 92
You plan to implement sensitivity labels for Microsoft Teams.
You need to ensure that you can view and apply sensitivity labels to new Microsoft Teams sites.
What should you do first?

A. Run the Set-sposite cmdlet.

B. Configure the EnableMTPLabels Azure Active Directory (Azure AD) setting.
C. Create a new sensitivity label scoped to Groups & sites.
D. Run the Execute-AzureAdLabelSync cmdtet.

Answer: C
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide

QUESTION 93
Your company has a Microsoft 365 tenant that uses a domain named contoso.
The company uses Microsoft Office 365 Message Encryption (OMI) to encrypt email sent to users in fabrikam.com.
A user named User1 erroneously sends an email to user2@fabrikam.
You need to disable user2@fabrikam.com from accessing the email.
What should you do?

A. Run the New-ComplianceSearchAction cmdlet.
B. Instruct User1 to delete the email from her Sent Items folder from Microsoft Outlook.
C. Run the Get-MessageTrace Cmdlet.
D. Run the Set-OMEMessageRevocation Cmdlet.
E. instruct User1 to select Remove external access from Microsoft Outlook on the web.

Answer: C

QUESTION 94
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 AssessmentTemplate.docx.
B. Create a sensitive info type that uses Exact Data Match (EDM).
C. Create a fingerprint of 100 sample documents in the Assessments folder.
D. Import 100 sample documents from the Assessments folder to a seed folder.

Answer: D

QUESTION 95
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 that uses the following sensitivity labels:
* Confidential
* Internal
* External
The labels are published by using a label policy named Policy1. Users report that Microsoft Office for the wen apps do not display the Sensitivity button. The Sensitivity button appears in Microsoft 365 Apps that are installed locally.
You need to ensure that the users can apply sensitivity labels to content when they use Office for the web apps.
Solution: You modify the publishing settings of Policy1.

Does the meet the goal?

A. Yes
B. No

Answer: B

QUESTION 96
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 that uses the following sensitivity labels:
* Confidential
* Internal
* External
The labels are published by using a label policy named Policy1. Users report that Microsoft Office for the wen apps do not display the Sensitivity button. The Sensitivity button appears in Microsoft 365 Apps that are installed locally.
You need to ensure that the users can apply sensitivity labels to content when they use Office for the web apps.
Solution: You modify the scope of the Confidential label.
Does this meet the goal?

A. Yes
B. No

Answer: B

QUESTION 97
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 that uses the following sensitivity labels:
* Confidential
* Internal
* External
The labels are published by using a label policy named Policy1. Users report that Microsoft Office for the wen apps do not display the Sensitivity button. The Sensitivity button appears in Microsoft 365 Apps that are installed locally.
You need to ensure that the users can apply sensitivity labels to content when they use Office for the web apps.
Solution: You run the Execute-AzureAdLabelSync cmdlet.
Does this meet the goal?

A. Yes
B. No

Answer: A

QUESTION 98
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 onboard the computers to Microsoft Defender fur Endpoint.
Does this meet the goal?

A. Yes
B. No

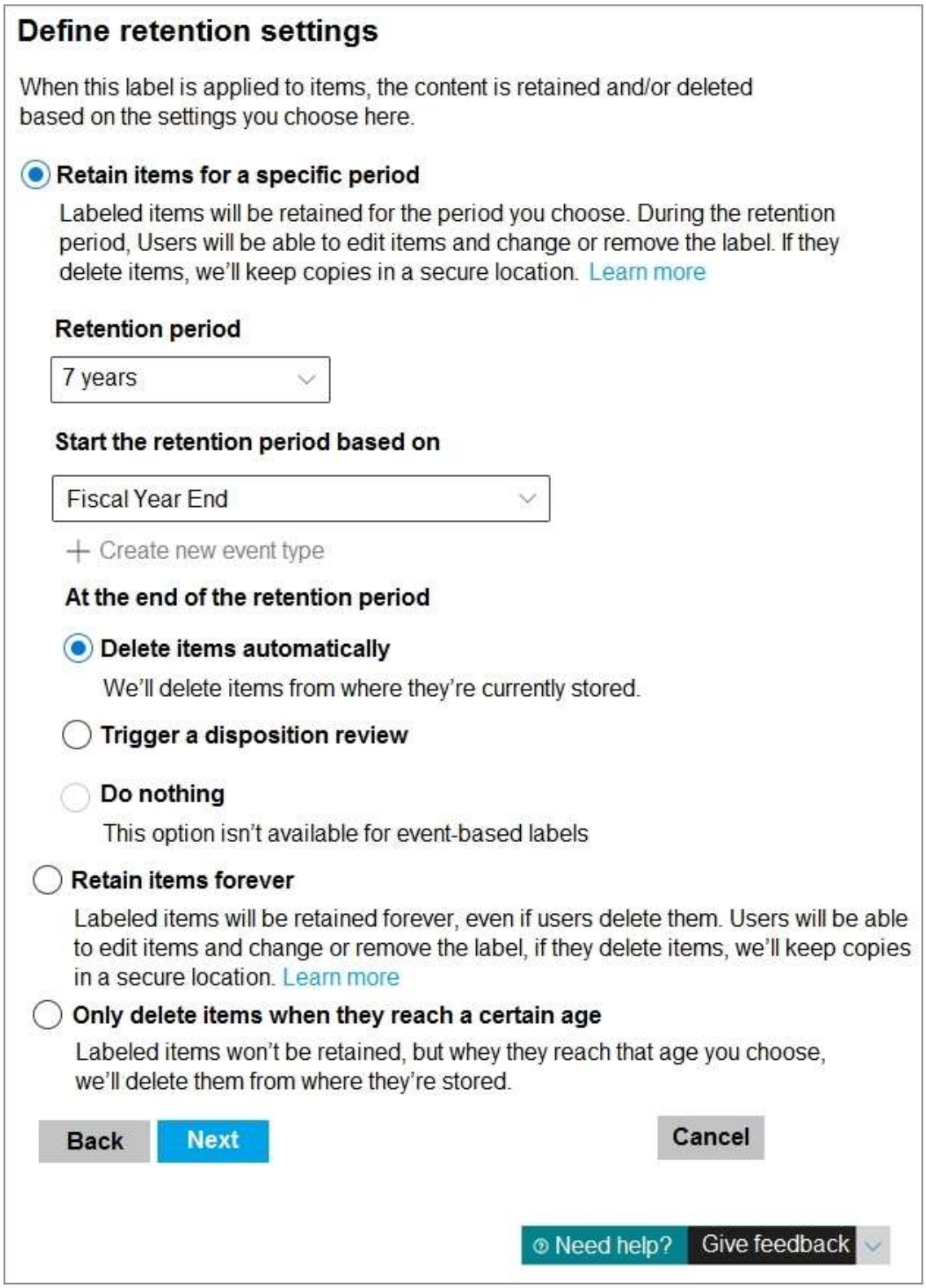
Answer: A

QUESTION 99
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 enroll the computers in Microsoft intune.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started?view=o365-worldwide

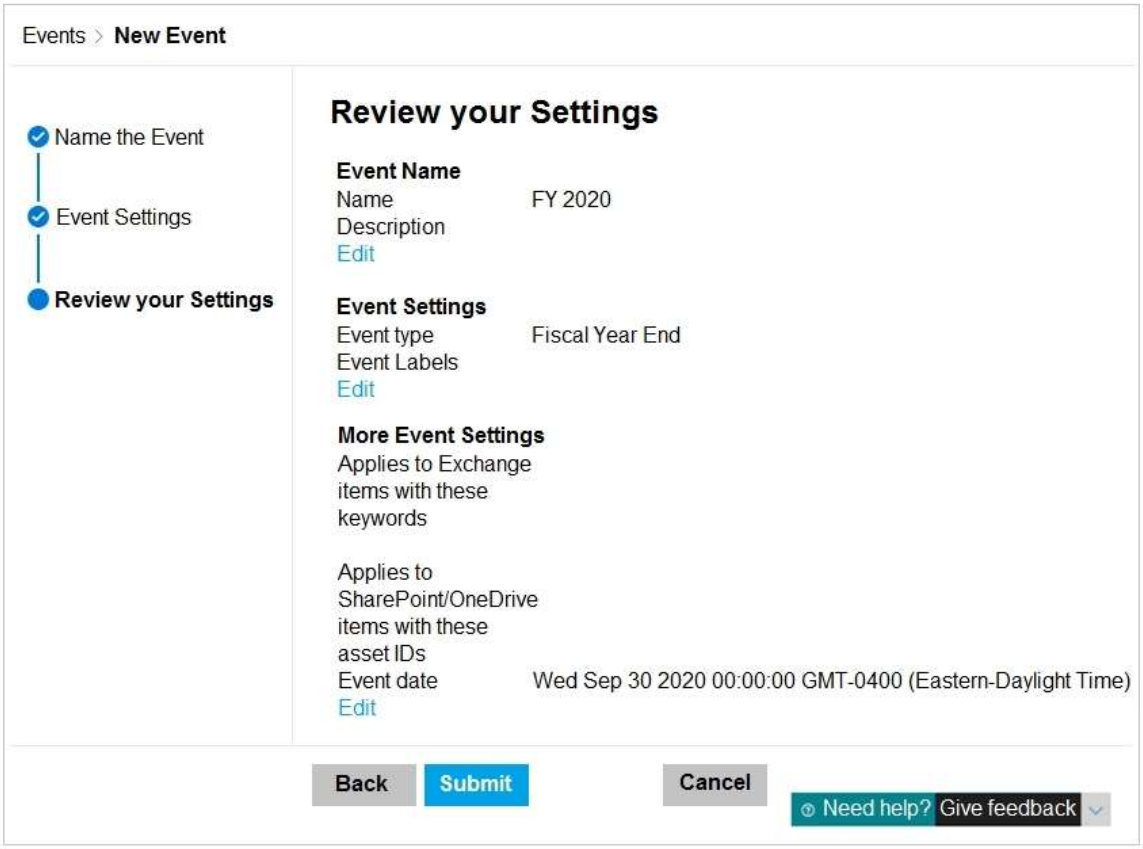
QUESTION 100
Hotspot Question
You have the retention label policy shown in the Policy exhibit. (Click the Policy tab.)



Users apply the retention label policy to files and set the asset ID as shown in the following table.

File name	Creation date	Asset ID
Doc1.docx	September 1, 2020	FY20
Doc2.docx	September 20, 2020	FY20
Doc3.docx	October 15, 2020	FY21

On December 1. 2020. you create the event shown in the Event exhibit. (Click the Event tab.):



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

Answer Area

Statements	Yes	No
Doc1.docx will be retained until December 30, 2027.	○	○
Doc2.docx will be retained until September 30, 2027.	○	○
Doc3.docx will be retained until September 30, 2027.	○	○

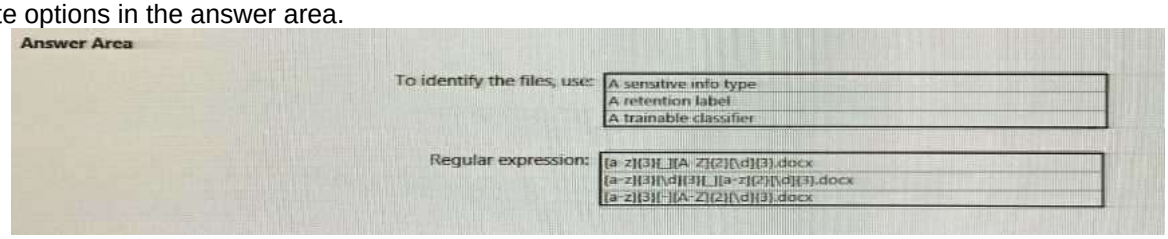
Answer:

Answer Area

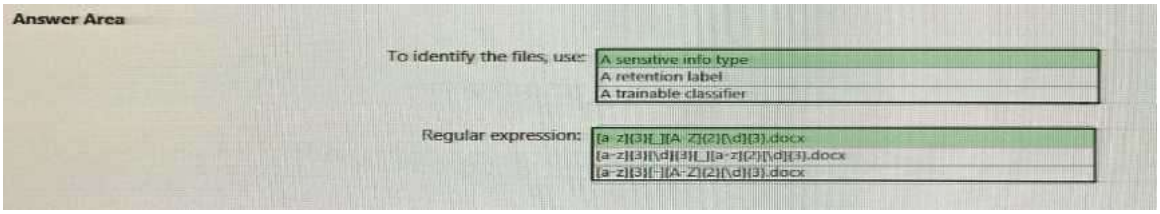
Statements	Yes	No
Doc1.docx will be retained until December 30, 2027.	○	○
Doc2.docx will be retained until September 30, 2027.	○	○
Doc3.docx will be retained until September 30, 2027.	○	○

QUESTION 101
Hotspot Question
At the end of a project you upload project documents to a Microsoft SharePoint Online library that contains many fifes.
Files that have the following naming format must be labeled as Project Documents:
- aei_AA989.docx
- bci_WS098.docx
- cei_DF112.docx
- ebc_QQ454.docx
- ecc_BB565.docx

You plan to create an auto-apply retention label policy.
What should you use to identify the files, and which regular expression should you use? To answer, select the appropriate options in the answer area.

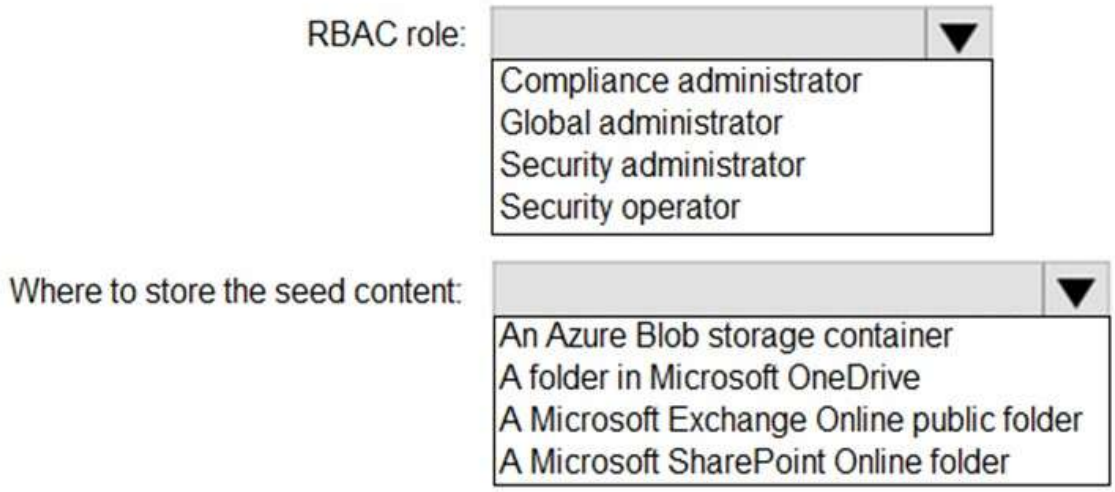


Answer:



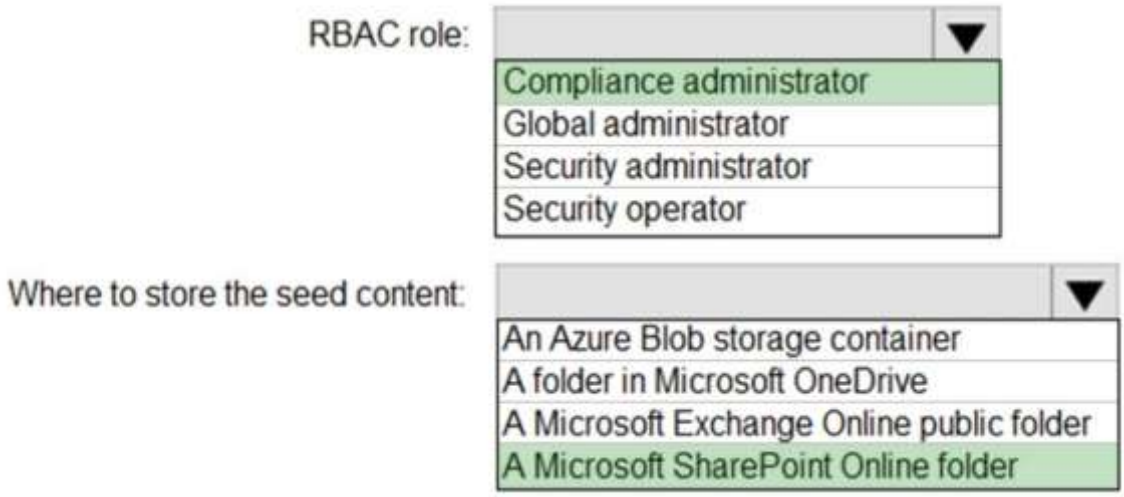
QUESTION 102
Hotspot Question
You plan to create a custom trainable classifier based on an organizational form template.
You need to identity which role based access control (RBAC) role is required to create the trainable classifier and where to classifier.
The solution must use the principle of least privilege.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

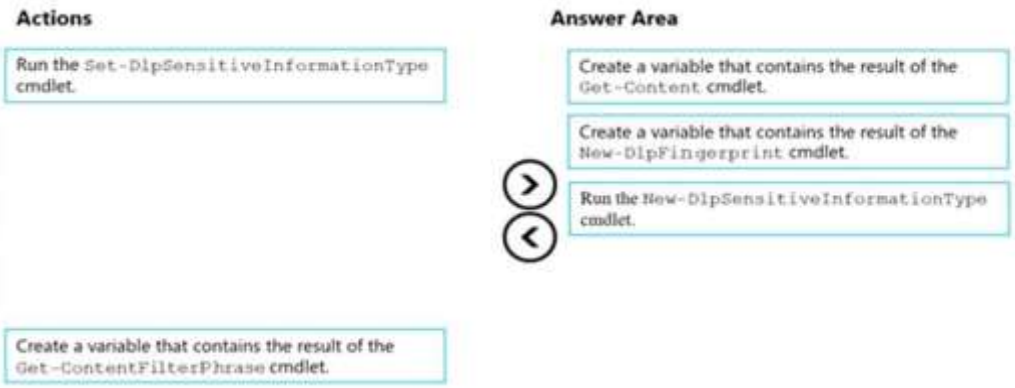
Answer Area



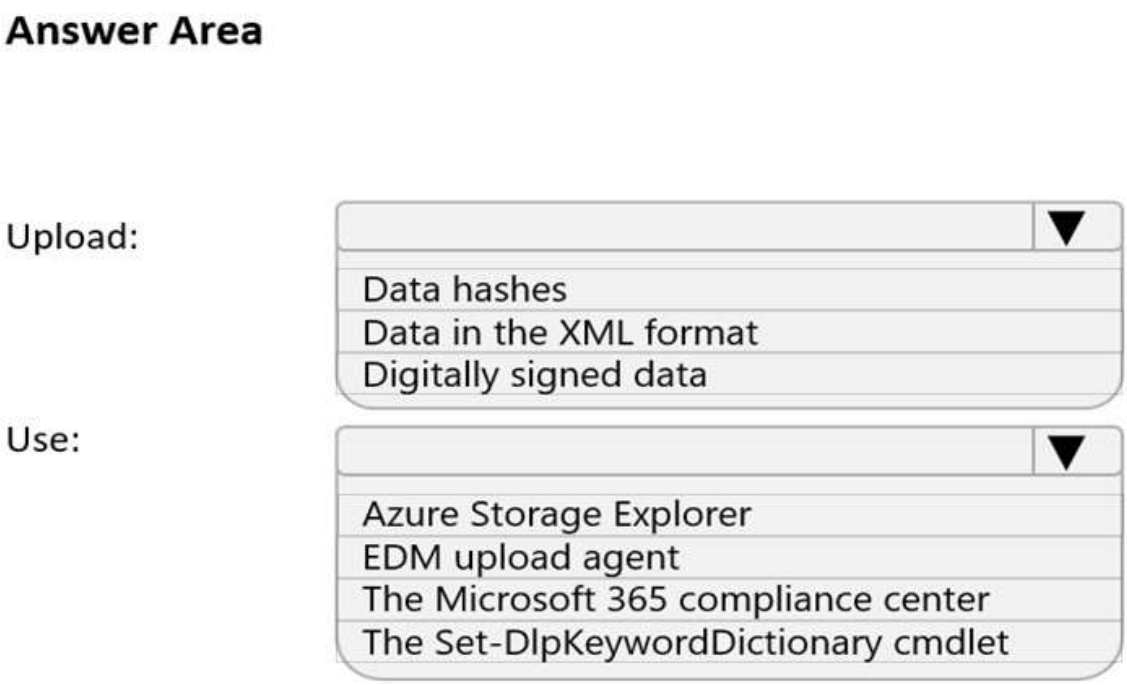
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide#prepare-for-a-custom-trainable-classifier

QUESTION 103
Drag and Drop Question
You have a Microsoft 365 tenant that uses data loss prevention (DLP).
You have a custom employee information form named Template 1.docx.
You need to create a classification rule package based on the document fingerprint of Templatel.docx.
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.

Answer:

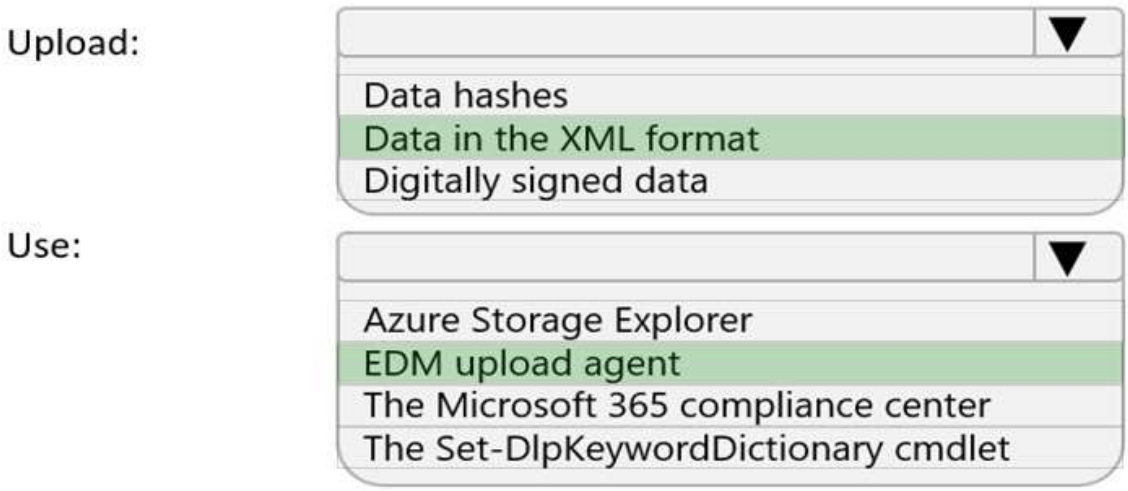


QUESTION 104
Hotspot Question
You plan to create a custom sensitive information type that will use Exact Data Match (EDM).
You need to identify what to upload to Microsoft 365, and which tool to use for the upload.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

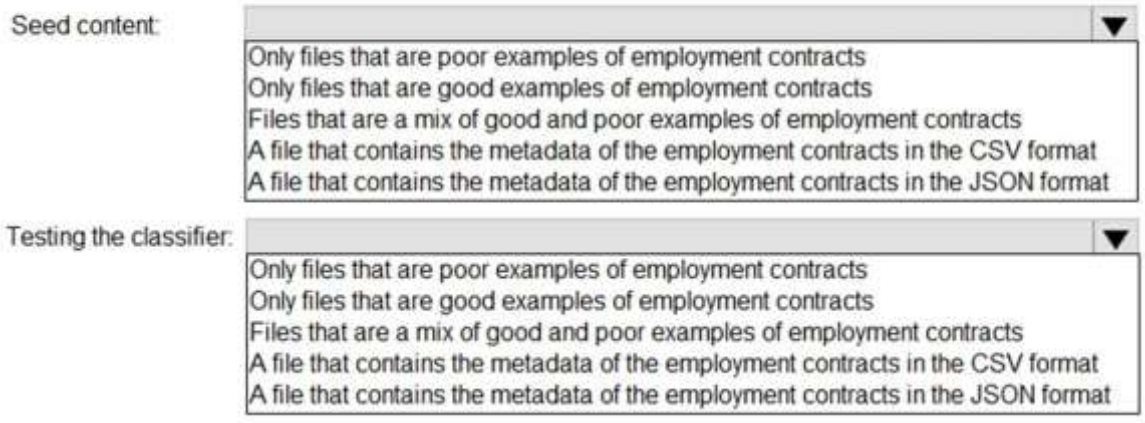
Answer Area



Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-custom-sensitive-information-types-with-exact-data-match-based-classification?view=o365-worldwide

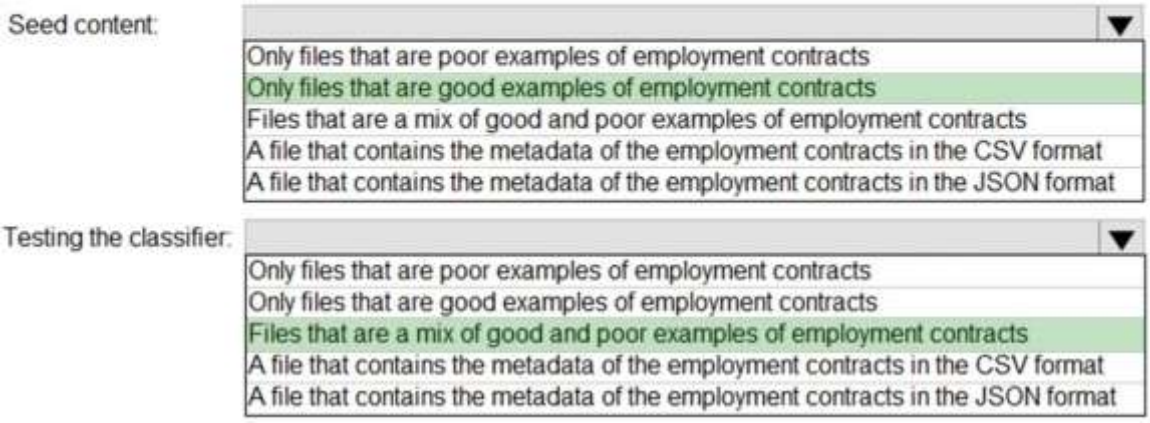
QUESTION 105
Hotspot Question
You plan to implement a sensitive information type based on a trainable classifier.
The sensitive information type will identify employment contracts.
You need to copy the required files to Microsoft SharePoint Online folders to train the classifier.
What should you use to seed content and test the classifier? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



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

QUESTION 106
You have a Microsoft 365 tenant that uses Microsoft Office 365 Message Encryption (OME).
You need to ensure that any emails containing attachments and sent to user1@contoso.com are encrypted automatically by using OME.
What should you do?

A. From the Exchange admin center, create a new sharing policy.
B. From the Microsoft 365 security center, create a Safe Attachments policy.
C. From the Exchange admin center, create a mail flow rule.
D. From the Microsoft 365 compliance center, configure an auto-apply retention label policy.

Answer: C
Explanation:
You can create mail flow rules to help protect email messages you send and receive.
You can set up rules to encrypt any outgoing email messages and remove encryption from encrypted messages coming from inside your organization or from replies to encrypted messages sent from your organization.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/define-mail-flow-rules-to-encrypt-email?view=o365-worldwide

QUESTION 107
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

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

QUESTION 108

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. Used and User2 only
B. Used and User4 only
C. Used, User2, User3, and User4
D. Used only
E. Used and User3 only

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

QUESTION 109
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. Device 1, Device2, Device3, Device4, and Device5
D. Device3 and Device4 only
E. Device1 and Device2 only

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

QUESTION 110
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

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

QUESTION 111
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

Answer: B
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 112
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

Answer: B
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 113
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

Answer: A
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 114
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

Answer: B
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 115
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

Answer: D
Explanation:
File plan in Records management allows you to bulk-create retention labels by importing the relevant information from a spreadsheet.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/file-plan-manager?view=o365-worldwide

QUESTION 116
You have a Microsoft 365 tenant.
You discover that email does NOT use Microsoft Office 365 Message Encryption (OME).
You need to ensure that OME can be applied to email.
What should you do first?

A. Enable Microsoft Defender for Office 365.
B. Activate Azure Information Protection.
C. Activate Azure Rights Management (Azure RMS).
D. Create an Azure key vault.

Answer: C
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/set-up-new-message-encryption-capabilities?view=o365-worldwide

QUESTION 117
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

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

QUESTION 118
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 files automatically
C. a retention policy that deletes files automatically
D. a retention label policy of type auto-apply

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

QUESTION 119
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 to 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. False positive and override
B. Third-party DLP policy matches
C. DLP policy matches
D. DLP incidents

Answer: C