
**Vendor:**Microsoft

**Exam Code:**SC-400

**Exam Name:**Microsoft Information Protection Administrator

**Version:**Demo

**QUESTION 1**

You need to test Microsoft Office 365 Message Encryption (OME) capabilities for your company. The test must verify the following information:

1.

The acquired default template names

2.

The encryption and decryption verification status Which PowerShell cmdlet should you run?

A. Test-ClientAccessRule

B. Test-Mailflow

C. Test-OAuthConnectivity

D. Test-IRMConfiguration

Correct Answer: D

Reference:

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

---

**QUESTION 2**

HOTSPOT

You have a Microsoft 365 subscription that contains a Microsoft SharePoint site named Site1. For Site1, users are assigned the roles shown in the following table.

| Name | Role |
|---|---|
| User1 | Owner |
| User2 | Member |

You publish retention labels to Site1 as shown in the following table.

| Name | Retention period | During the retention period |
|---|---|---|
| Retention1 | 5 years | Mark items as a record |
| Retention2 | 5 years | Mark items as a regulatory record |

You publish retention labels to Site1 as shown in the following table. You have the files shown in the following table.

| Name | Applied retention label |
|---|---|
| File1 | Retention1 |
| File2 | Retention2 |

For each of the following statement, 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 delete File2. | ○ | ○ |
| User2 can rename File1. | ○ | ○ |
| User1 can apply Retention2 to File1. | ○ | ○ |

Correct Answer:

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| User1 can delete File2. | ○ | ○ |
| User2 can rename File1. | ○ | ○ |
| User1 can apply Retention2 to File1. | ○ | ○ |

---

**QUESTION 3**

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 for Endpoint.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

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

---

**QUESTION 4**

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 Defender for Cloud Apps, you mark the application as Unsanctioned.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Explanation:

Sanctioning/unsanctioning an app

You can unsanction a specific risky app by clicking the three dots at the end of the row. Then select Unsanction. Unsanctioning an app doesn\\'t block use, but enables you to more easily monitor its use with the Cloud Discovery filters. You can

then notify users of the unsanctioned app and suggest an alternative safe app for their use, or generate a block script using the Defender for Cloud Apps APIs to block all unsanctioned apps.

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

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

Reference: https://learn.microsoft.com/en-us/defender-cloud-apps/governance-discovery#BKMK_SanctionApp

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

---

**QUESTION 5**

You have a Microsoft 365 tenant that uses the following sensitivity labels:

1.

Confidential

2.

Internal

3.

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

Correct Answer: A

---

**QUESTION 6**

You plan to create a new data loss prevention (DLP) policy named DIP1.

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

https://learn.microsoft.com/en-us/purview/dlp-policy-reference#policy-scoping

---

**QUESTION 7**

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: CD

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

---

**QUESTION 8**

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

Correct Answer: B

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

---

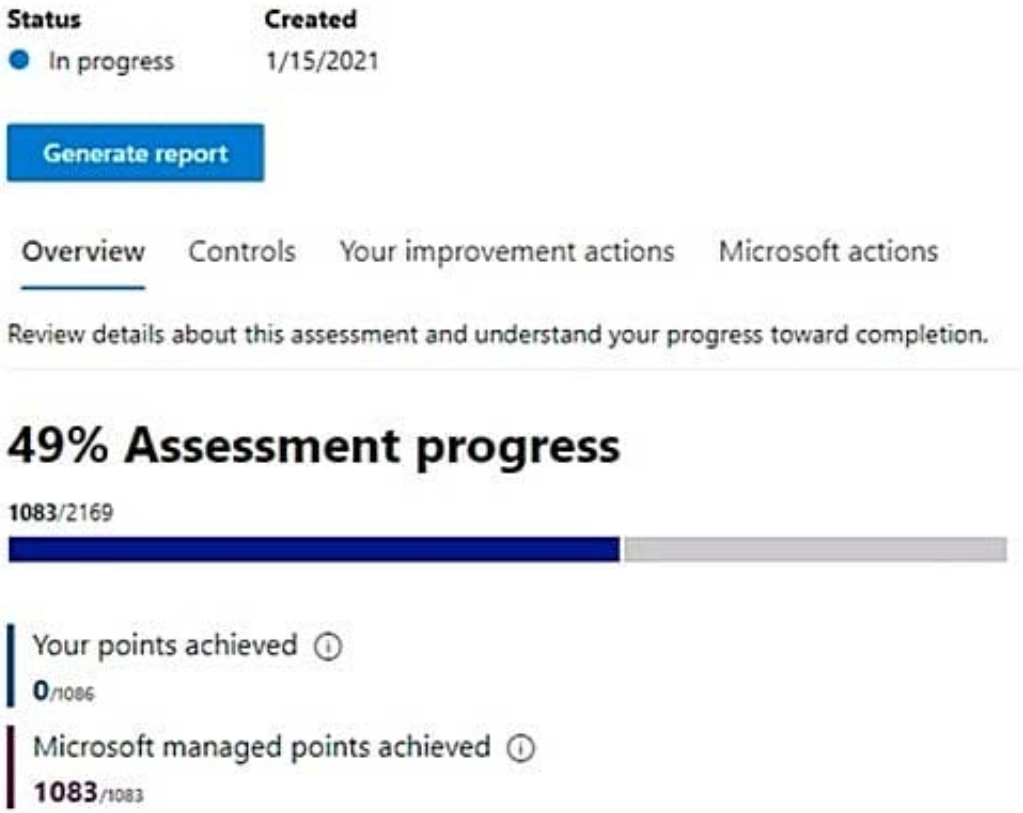
**QUESTION 9**

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.




Which users can update the title of Assessment1, 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

Correct Answer:

**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

---

**QUESTION 10**

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

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 11**

HOTSPOT

You have a Microsoft 365 tenant named contoso.com that contains two users named User1 and User2. The tenant uses Microsoft Office 365 Message Encryption (OME).

User1 plans to send emails that contain attachments as shown in the following table.

| Subject | To | Attachment type | Message size |
|---|---|---|---|
| Mail1 | User2@contoso.com | .docx | 40 MB |
| Mail2 | User4@outlook.com | .doc | 3 MB |
| Mail3 | User3@gmail.com | .xlsx | 7 MB |

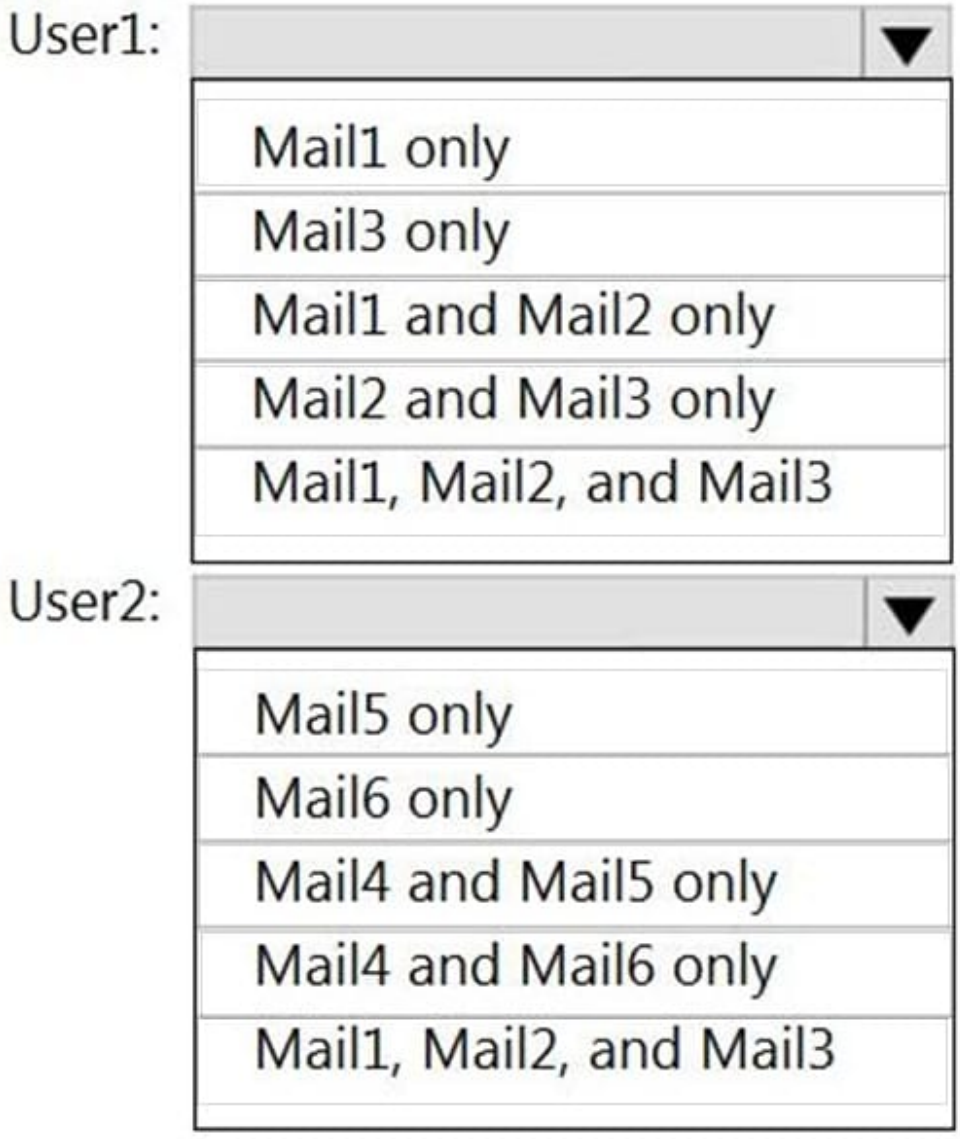
User2 plans to send emails that contain attachments as shown in the following table.

| Subject | To | Attachment type | Message size |
|---|---|---|---|
| Mail4 | User1@contoso.com | .pptx | 4 MB |
| Mail5 | User4@outlook.com | .jpg | 6 MB |
| Mail6 | User3@gmail.com | .docx | 3 MB |

For which emails will the attachments be protected? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

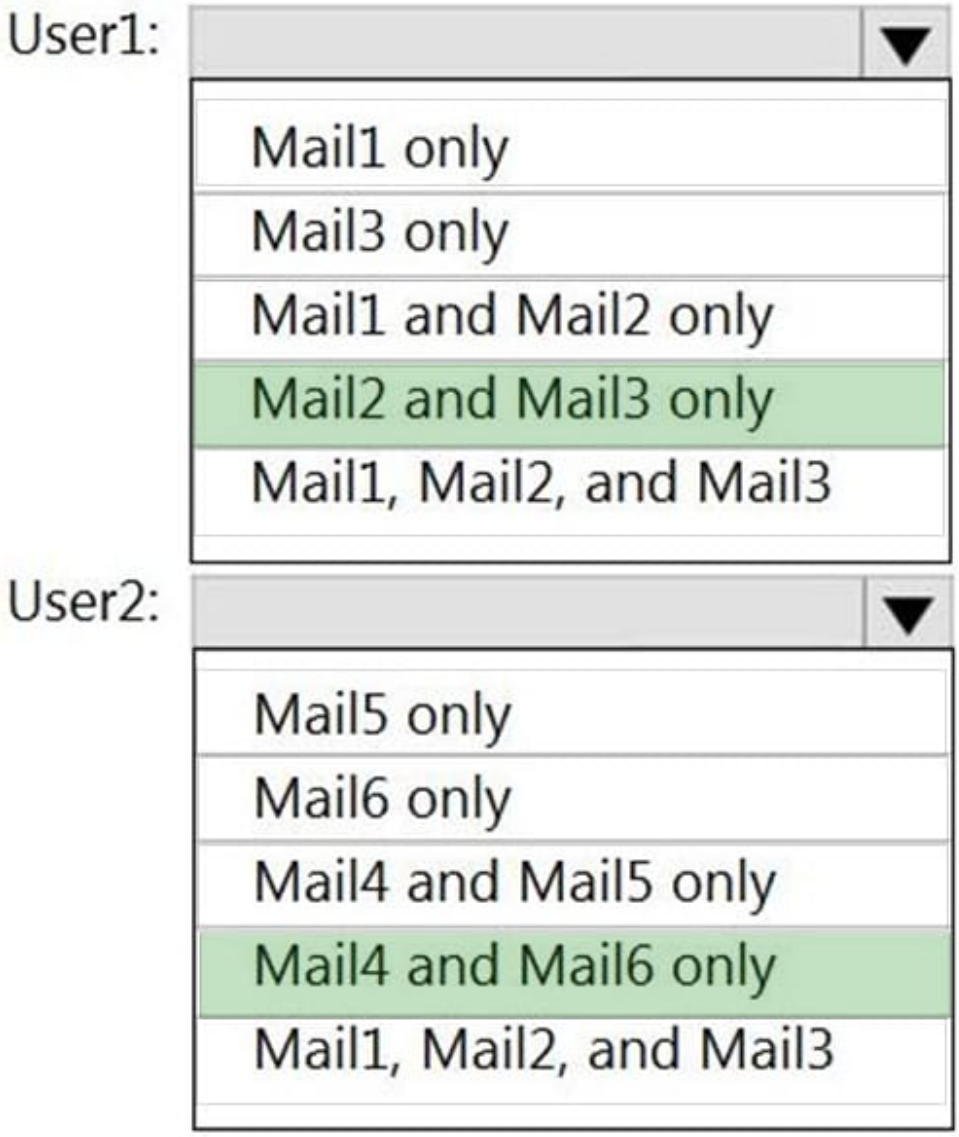
Hot Area:

**Answer Area**




Correct Answer:

## Answer Area




---

**QUESTION 12**

HOTSPOT

You have a Microsoft 365 E5 subscription.

You have the data loss prevention (DLP) rule match shown in the following exhibit.

# DLP rule matched

## Activity details

Activity
DLP rule matched

Happened
May 30, 2022 8:25 PM

## About this item

File
FW: Doc1.docx

User
user1@contoso.com

File size
1.4 MB

Sensitive info type
Credit Card Number

DLP policy
Financial Data

DLP rule
Financial Data - High Volume

Policy mode
Enable

Rule actions
ExModerate

Email subject
FW: Doc1.docx

Email sender
user1@contoso.com

Email recipient
user2@fabrikam.com

## Location details

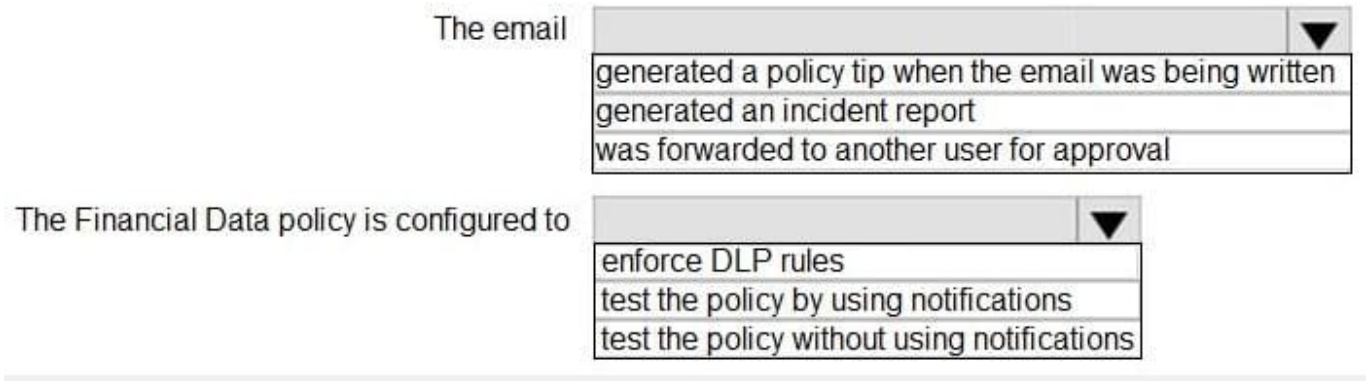
Location
Exchange

Parent
FW: Doc1.docx

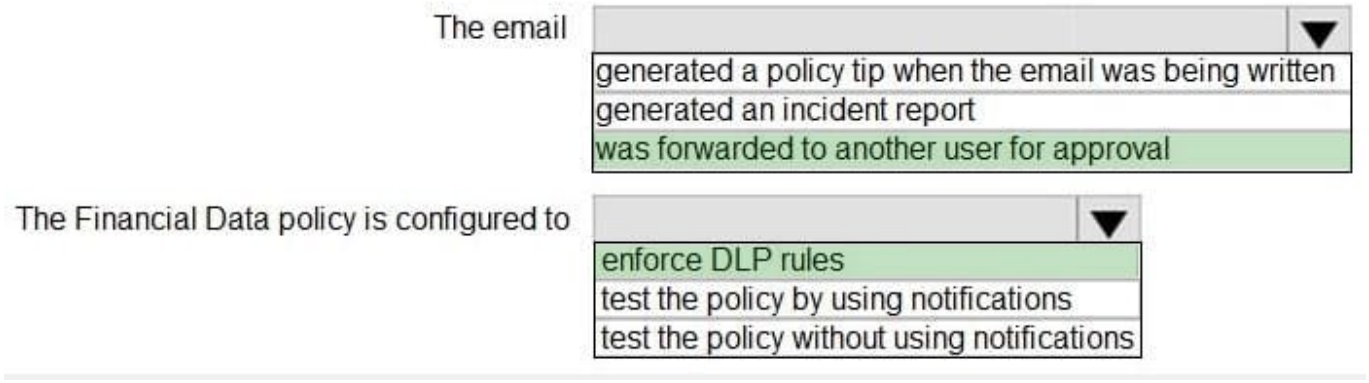
File path
FW: Doc1.docx

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:




Correct Answer:




Explanation:

Box 1: Was forwarded to another user for approval

We see Rule actions: ExModerate.

The "moderation" feature we are using is the DLP Action "Forward the message for approval to specific approvers".

The term "moderation" comes from the "ExModerate" Rule Action that is shown in the DLP event Activity Details screen in the Data Loss Prevention Activities Explorer. See attached DLP exmoderate screenshot to see how this looks in my tenant.

As you can see from the Activity Details, you are unable to see the result of the ExModerate Rule Action. Did the approver approve or deny the message? I cannot see that in the Activity Details.

Box 2: enforce DLP rules

Policy mode is enabled.

Reference: https://techcommunity.microsoft.com/t5/exchange/exchange-unified-dlp-moderation-logging-and-reporting/m-

p/2416894