



Microsoft AB-650 Dumps

Shared by Puckett on 19-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

AB-650 Mix Questions IN THIS CASE STUDY

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft 365 subscription that contains Microsoft 365 Copilot agents deployed to multiple departments at your company.

The adoption team reports team reports increasing license assignments, and corporate management wants to identify Copilot engagement gaps by Microsoft 365 apps and features.

You need to provide the required adoption insights. The solution must support targeted user education without using audit events or prompt content.

Solution: From the Microsoft 365 admin center, you review the Microsoft 365 Copilot usage report.

Does this meet the goal?

Options:

A- Yes

B- No

Answer:

A

Explanation:

The Microsoft 365 Copilot usage report provides detailed adoption and engagement metrics that enable administrators to evaluate how effectively licensed users utilize Copilot across Microsoft 365 applications.

Option A is correct because the report supports the required analysis without relying on Microsoft Purview audit events or examining the content of user prompts.

Administrators can access the report through Microsoft 365 admin center Reports Usage Microsoft Copilot Copilot Usage.

The report provides several relevant metrics, including enabled users, active users, active-user rates, adoption trends, and application-specific activity across Word, Excel, PowerPoint, Outlook, Teams, and other supported applications.

The Adoption by app section enables administrators to compare licensed users against active Copilot users in each application. This helps identify applications where license deployment is increasing but actual engagement remains low.

The report also tracks supported Copilot feature interactions, enabling administrators to understand usage patterns and identify opportunities for targeted training.

For example, low adoption in Excel may indicate a need for training on AI-assisted data analysis, while low Teams engagement may indicate limited awareness of meeting summarization capabilities.

Microsoft specifically recommends using official Copilot usage reports rather than audit logs for adoption measurement because the reporting metrics are designed for consistent usage analysis.

Therefore, reviewing the Microsoft 365 Copilot usage report meets the stated goal.

Question 2

Question Type: Hotspot

Case Study: Mix Questions

Mix Questions

AB-650 Mix Questions IN THIS CASE STUDY

You have a Microsoft 365 E5 subscription that contains a user named Admin1.

Your company deploys a new branch office named Branch1.

You need to provide Admin1 with the ability to manage Branch1. The solution must meet the following requirements:

Admin1 must only be able to manage users that have Office location set to Branch1.

Admin1 must be able to reset passwords, manage user licenses, and modify user attributes only for the users in Branch1.

What should you use to organize the Branch1 users, and which role should you assign to Admin1?
To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Use:

	▼
An administrator unit	
A Microsoft 365 group	
A security group	

Role:

	▼
Help Desk Administrator	
Password Administrator	
User Administrator	

Answer:

See the Answer in the Premium Version!

Question 3

Question Type: Hotspot

Case Study: Mix Questions

Mix Questions

AB-650 Mix Questions IN THIS CASE STUDY

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

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group2

AntiSpam1

Name: AntiSpam1

Priority: 0

Include these users, groups and domains

Users: User3

Groups: Group1

Exclude these users, groups and domains

Groups: Group2

Message limits

Set a daily message limit: 100

AntiSpam2

Name: AntiSpam2

Priority: 1

Include these users, groups and domains

Users: User1

Groups: Group2

Exclude these users, groups and domains

Users: User3

Message limits

Set a daily message limit: 50

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
User1 can send a maximum of 150 email messages per day.	☐	☐
User2 can send a maximum of 50 email messages per day.	☐	☐
User3 can send a maximum of 100 email messages per day.	☐	☐

Answer:

See the Answer in the Premium Version!

Question 4

Question Type: Hotspot

Case Study: Mix Questions

Mix Questions

AB-650 Mix Questions IN THIS CASE STUDY

You have a Microsoft 365 E5 tenant.

You have a sensitivity label configured as shown in the Sensitivity label exhibit. (Click the Sensitivity label tab.)

You have an auto-labeling policy as shown in the Auto-labeling policy exhibit. (Click the Auto-labeling policy tab.)

A user sends an email that contains the components shown in the following table.

Type	File	Includes IP address
Mail body	<i>Not applicable</i>	No
Attachment	File1.docx	Yes
Attachment	File2.xml	Yes

Review your settings and finish

Name

Sensitivity1

[Edit](#)

Display name

Sensitivity1

[Edit](#)

Description for users

Sensitivity1

[Edit](#)

Scope

File, Email

[Edit](#)

Access control

None

[Edit](#)

Content marking

Watermark: Watermark

Header: Header

[Edit](#)

Auto-labeling for files and emails

None

[Edit](#)

Auto-labeling for schematized data assets (preview)

None

[Edit](#)



Review and finish

Policy name

Auto-labeling policy

[Edit](#)

Label and policy settings

Label Sensitivity1

Exchange overwrite label false

[Edit](#)

Policy template type

Custom policy

[Edit](#)

Sensitive Info Type

IP Address

Trainable Classifier

Admin units

None

Apply to content in these locations

Exchange email All

[Edit](#)

Exclude content from these locations

Exchange email None

[Edit](#)

Rules for auto-applying this label

Exchange email 1 rule

[Edit](#)

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
Sensitivity1 is applied to the email	☐	☐
A watermark is added to File1.docx	☐	☐
A header is added to File2.xml	☐	☐

Answer:

See the Answer in the Premium Version!

Question 5

Question Type: Hotspot

Case Study: Mix Questions

Mix Questions

AB-650 Mix Questions IN THIS CASE STUDY

You have a Microsoft 365 subscription that contains three users named User1, User2, and User3.

The subscription has Conditional Access policies assigned to all users. The policies are configured as shown in the following table.

Name	Target resources	Conditions	Access controls
CA1	All resources	Client apps: Any client app	Grant access: Require multifactor authentication
CA2	Office 365 Exchange Online	Client apps: Exchange ActiveSync and Other clients	Block access
CA3	Office 365 SharePoint Online	Client apps: Any client app	Grant access: Require device to be marked as compliant

The users report that they fail to access Microsoft 365 resources as shown in the following table.

User	Resource	From client app
User1	Microsoft Teams	Microsoft Edge
User2	Microsoft Exchange	Exchange ActiveSync
User3	Microsoft SharePoint	Google Chrome

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

User2 can access Exchange by switching to Microsoft Outlook

☐
☐

User1 must complete multifactor authentication (MFA) to access Teams

☐
☐

User3 can access SharePoint by switching to Microsoft Edge on the same device

☐
☐

Answer:

See the Answer in the Premium Version!

Question 6

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

AB-650 Mix Questions IN THIS CASE STUDY

You have a Microsoft 365 subscription.

You need to create a data loss prevention (DLP) policy that is configured to use the Set headers action.

To which location can the policy be applied?

Options:

- A- OneDrive accounts
- B- Exchange email
- C- SharePoint sites
- D- Teams chat and channel messages

Answer:

B

Explanation:

Microsoft Purview Data Loss Prevention (DLP) policies support different actions depending on the Microsoft 365 workload to which a policy is applied. Administrators must select a supported location before configuring a particular DLP action.

Option B is correct because the Set headers action is supported specifically for Exchange Online email.

This action allows administrators to add or modify an email message header when the message matches the conditions of a DLP rule. For example, an organization can configure a rule that detects sensitive financial information and adds a custom header indicating that the email requires additional handling.

Microsoft documents Set headers as a non-halting action, meaning it does not automatically stop subsequent DLP rule processing.

Option A is incorrect because OneDrive policies govern files and sharing activities rather than Exchange transport message headers.

Option C is incorrect because SharePoint DLP policies primarily protect stored documents and control access to sensitive content.

Option D is incorrect because Teams chat and channel messages do not expose the Exchange-specific Set headers action.

Therefore, the DLP policy must include the Exchange email location to support Set headers.

Microsoft Reference: [Microsoft Learn --- Data Loss Prevention policy reference.](#)

Question 7

Question Type: Hotspot

Case Study: Mix Questions

Mix Questions

AB-650 Mix Questions IN THIS CASE STUDY

You have a Microsoft 365 subscription that contains two security groups named Group1 and Group2. Group2 is a member of Group1. The subscription contains the users shown in the following table.

Name	Description
User1	User in Group2 that has no authentication methods registered
User2	User in Group1 that has only a mobile phone authentication method registered
User3	User in Group1 that has email and mobile phone authentication methods registered

The subscription has self-service password reset (SSPR) enabled as shown in the following table.

Setting	Value
Self service password reset enabled	Selected: Group1
Number of methods required to reset	2
Methods available to users	Email, Mobile phone, and Mobile app notification

User3 failed mobile phone authentication six times during the last 50 minutes. 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

User2 can complete a password reset.

☐
☐

User3 can use email to reset their password immediately

☐
☐

User1 is eligible for SSPR registration through group-based enablement

☐
☐

Answer:

See the Answer in the Premium Version!

Question 8

Question Type: Hotspot

Case Study: Mix Questions

Mix Questions

AB-650 Mix Questions IN THIS CASE STUDY

You have a Microsoft 365 subscription that uses Privileged Identity Management (PIM).

A group of support engineers requires access to the User Administrator role in Microsoft Entra.

You need to configure privileged access for the engineers. The solution must meet the following requirements:

The engineers must activate the role before receiving user administrator privileges.

The engineers must complete multifactor authentication (MFA) during role activation.

A designated approver must authorize each activation request.

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

NOTE: Each correct selection is worth one point.

Answer Area

PIM assignment:

	▼
Active assignment	
Eligible assignment	
Permanent active assignment	
Time-bound active assignment	

PIM activation requirements:

	▼
Require approval and ticket information	
Require approval and multifactor authentication (MFA)	
Require justification and multifactor authentication (MFA)	
Require assignment expiration and multifactor authentication (MFA)	

Answer:

See the Answer in the Premium Version!

Question 9

Question Type: Hotspot

Case Study: Mix Questions

Mix Questions

AB-650 Mix Questions IN THIS CASE STUDY

You have a Microsoft Entra tenant that contains a cloud app named Payroll and three groups named Group1, Group2, and Group3.

Group2 is a member of Group1.

The subscription contains the users shown in the following table.

Name	Description
User1	User in Group2
User2	B2B collaboration guest user that is NOT in any groups
User3	User in Group1 and Group3

The subscription has the Conditional Access policies shown in the following table.

Name	Users and groups	Target resources	Access controls
CA1	Include: Group1 Exclude: Group3	Payroll	Grant access: Require multifactor authentication
CA2	Include all users Exclude: Group1 and Group3	Payroll	Block access

Answer Area

Statements

User2 is prevented from accessing Payroll

Yes

No

☐
☐

User1 must complete multifactor authentication (MFA) before accessing Payroll

☐
☐

User3 must complete multifactor authentication (MFA) before accessing Payroll

☐
☐

Answer:

See the Answer in the Premium Version!

Question 10

Question Type: Hotspot

Case Study: Mix Questions

Mix Questions

AB-650 Mix Questions IN THIS CASE STUDY

You have a Microsoft 365 E5 subscription.

You configure a new data loss prevention (DLP) policy named Policy1 that detects when sensitive content is shared externally.

Policy1 has the DLP rule shown in the following exhibit.

^ Conditions

We'll apply this policy to content that matches these conditions.

^ Content contains								
Group name *		Group operator						
Default		Any of these			▼			
Sensitive info types								
SWIFT Code	Medium confidence ▼	i	Instance count	1	to	9	i	🗑
EU Debit Card Number	High confidence ▼	i	Instance count	1	to	9	i	🗑
Credit Card Number	High confidence ▼	i	Instance count	1	to	9	i	🗑
Add ▼								

+ Add condition ▼

^ Exceptions

We won't apply this rule to content that matches any of these exceptions.

+ Add exception ▾

^ Actions

Use actions to protect content when the conditions are met.

+ Add an action ▾

^ User notifications

Use notifications to inform your users and help educate them on the proper use of sensitive info.

☒ On

i Support and behavior for policy tips varies across apps and platforms. [Learn where policy tips are supported](#)

Endpoint devices

☐ Show users a policy tip notification when an activity is restricted. This is turned on when you select Block for an activity in Windows. To turn off the notifications on Windows devices, disable the restrictions.

Microsoft 365 files and Microsoft Fabric items

☒ Notify users in Office 365 service with a policy tip or email notifications

Email notifications

[Preview and edit notification email](#)

☐ Notify the user who sent, shared, or last modified the content.

☒ Notify these people:

☒ The person who sent, shared, or modified the content

☒ Owner of the SharePoint site or OneDrive account

☒ Owner of the SharePoint or OneDrive content

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.

Answer Area

If a file matches the DLP rule of Policy1, the file will be [answer choice].

available to both internal and external users
encrypted
restricted from all users except the owner
restricted to internal users only

If 18 credit card numbers are detected in a file that is shared with external users, [answer choice] email notifications will be sent.

18
no
one
two

Answer:

See the Answer in the Premium Version!

Question 11

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

AB-650 Mix Questions IN THIS CASE STUDY

You have a Microsoft 365 subscription that contains a Microsoft Entra security group named Group1. The subscription has self-service password reset (SSPR) disabled.

You need to pilot SSPR for Group1. The solution must require users to use a mobile app notification to reset their password.

What should you configure in the Password reset settings?

Options:

- A- Authentication methods
- B- Administrator Policy
- C- Properties
- D- Registration
- E- Notifications

Answer:

A

Explanation:

Microsoft Entra self-service password reset (SSPR) allows users to reset their passwords without contacting an administrator or helpdesk. Administrators can configure which authentication methods users must complete to verify their identities.

Option A is correct because Authentication methods controls the verification methods available during password reset, including Microsoft Authenticator push notifications.

In the legacy SSPR configuration, administrators navigate to Microsoft Entra admin center Entra ID Password reset Authentication methods.

The Mobile app notification method allows users to verify their identities by responding to a Microsoft Authenticator notification.

An important configuration consideration is that the legacy SSPR experience supports app notifications when two authentication methods are required for password reset. When only one method is required, the mobile application verification code is supported instead.

To restrict the pilot to Group1, administrators must separately configure Properties, enable SSPR for selected users, and select Group1.

Option B configures administrator-specific password reset requirements. Option C controls SSPR enablement and targeting, but not the authentication method itself. Option D controls registration requirements, and Option E configures password reset notifications.

Current documentation qualification: Microsoft has deprecated management of authentication methods through legacy SSPR policies. For new deployments, administrators should configure Microsoft Authenticator through the centralized Authentication methods policy.

Question 12

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

AB-650 Mix Questions IN THIS CASE STUDY

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365. The subscription contains a group named Group1.

Group1 receives recurring unwanted email from countries where your company does NOT do business.

You need to reduce the unwanted email for Group1 without affecting other groups.

What should you configure?

Options:

- A- a connection filter policy
- B- the Strict preset security policy
- C- a custom anti-spam inbound policy
- D- the Standard preset security policy
- E- a custom anti-phishing policy

Answer:

C

Explanation:

Microsoft Defender for Office 365 provides configurable inbound anti-spam policies that enable administrators to filter unwanted email according to sender characteristics, geographic origin, languages, and recipient groups.

Option C is correct because a custom anti-spam inbound policy supports geographic filtering through the From these countries setting and can be scoped to selected recipient groups.

Administrators can configure the policy through the following steps:

Navigate to Microsoft Defender portal Email & collaboration Policies & rules Threat policies Anti-spam.

Select Create policy Inbound.

Under Users, groups, and domains, specify Group1 as the recipient group.

Under Bulk email threshold & spam properties, enable From these countries and select the countries or regions from which unwanted messages originate.

Configure the appropriate spam action, such as moving detected messages to Junk Email or quarantine.

This configuration ensures that geographic spam filtering applies specifically to Group1 without altering protection settings for other recipients.

Option A is incorrect because connection filter policies operate on source IP addresses and do not provide the required group-specific geographic filtering.

Options B and D are incorrect because preset security policies do not provide the required customizable country-based filtering settings.

Option E is incorrect because anti-phishing policies focus on spoofing, impersonation, and phishing detection rather than geographic spam filtering.

Implementation consideration: Recipient-group targeting supports mail-enabled security groups, distribution groups, and Microsoft 365 groups. Also, Standard or Strict preset security policies take precedence over custom inbound anti-spam policies for recipients included in those presets.



To Get Premium Files for AB-650 Visit

<https://www.p2pexams.com/products/ab-650>

For More Free Questions Visit

<https://www.p2pexams.com/microsoft/pdf/ab-650>

20%
DISCOUNT

P2P
exams