DUMPSARENA

Microsoft 365 Copilot and Agent Administration Fundamentals

Microsoft AB-900

Version Demo

Total Demo Questions: 10

Total Premium Questions: 65

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

You need to identify files and emails that contain social security numbers (SSNs) and credit card numbers. What should you use in the Microsoft Purview portal?

A. Information Protection reports

B. Data explorer

C. Information Protection policies

D. Activity explorer

ANSWER: B

Explanation:

Use **Data explorer**. In Microsoft Purview, Data explorer is designed to help you discover and understand where sensitive data exists across supported Microsoft 365 locations by showing a snapshot of items that have been classified (for example, by built-in *sensitive information types* such as U.S. Social Security Number and Credit Card Number). This directly matches the requirement to identify files and emails containing SSNs and credit card numbers.

The other choices don't fit the "find where this sensitive data exists" goal. **Information Protection reports** are primarily oriented around labeling and protection usage/reporting rather than inventorying content by sensitive info type. **Information Protection policies** are for configuring how labels and protection behave (classification, encryption, markings), not for locating existing content containing specific data patterns. **Activity explorer** focuses on auditing and investigating events (for example, DLP rule matches, label application/removal activities) rather than providing a discovery view of all items containing SSNs/credit card numbers.

References: Microsoft Purview Data explorer, Sensitive information types in Microsoft Purview.

QUESTION NO: 2

Your organization has a Microsoft 365 subscription.

You create a security group named Group1 and assign a Microsoft 365 E3 license to the group. You discover that a user named User1 does NOT have access to the Microsoft 365 E3 features. You need to ensure that User1 can access all the Microsoft 365 E3 features.

Which two actions can you perform? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Add User1 to Group1.

B. Assign a Conditional Access policy to Group1.

C. Assign a Conditional Access policy to User1.

D. Assign a license to User1.

ANSWER: A D

Explanation:

Correct answers: **A** and **D**.

With Microsoft Entra ID (Azure AD) group-based licensing, any user who is a member of a group that has a license assigned will inherit that license automatically (assuming licensing prerequisites are met, such as the user having a valid usage location and there being available licenses). Therefore, adding **User1** to **Group1** is a complete fix because it causes the Microsoft 365 E3 license to be applied through group membership.

Alternatively, you can bypass group-based licensing entirely and assign the Microsoft 365 E3 license **directly to User1**. Direct user licensing is supported and immediately grants the entitlements associated with the license (again, subject to prerequisites like usage location and license availability). Either approach ensures User1 receives the Microsoft 365 E3 service plan entitlements.

Options **B** and **C** are incorrect because Conditional Access controls *how* and *under what conditions* a user can access cloud apps after authentication; it does not grant product entitlements or assign licenses. If a user isn't licensed for Microsoft 365 E3, Conditional Access can't make E3 features available.

References: Group-based licensing in Microsoft Entra ID, Assign licenses to users in Microsoft 365

QUESTION NO: 3 - (HOTSPOT)

HOTSPOT

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:

Explanation:

This hotspot is testing basic SharePoint site permissions and what “Members” and “Owners” can do. For the first statement, SharePoint sharing is typically available to site users (including Members) unless an admin or site owner has restricted sharing. When a member shares a site or content, SharePoint can either grant access directly or generate an access request that an owner approves, depending on how the site is configured. In fundamentals-style questions, the key idea is that members can invite/share with others in many common configurations, so the statement is treated as true. Microsoft describes how sharing and access requests work in SharePoint here: Share a site or folder in SharePoint.

For the second statement, SharePoint permissions can be assigned not only to individual users but also to groups. A Microsoft 365 group can be granted access to a SharePoint site by adding it to a SharePoint group such as Members (or Visitors/Owners as appropriate). This aligns with Microsoft guidance on managing site permissions and adding users/groups to SharePoint groups: Manage site permissions in SharePoint.

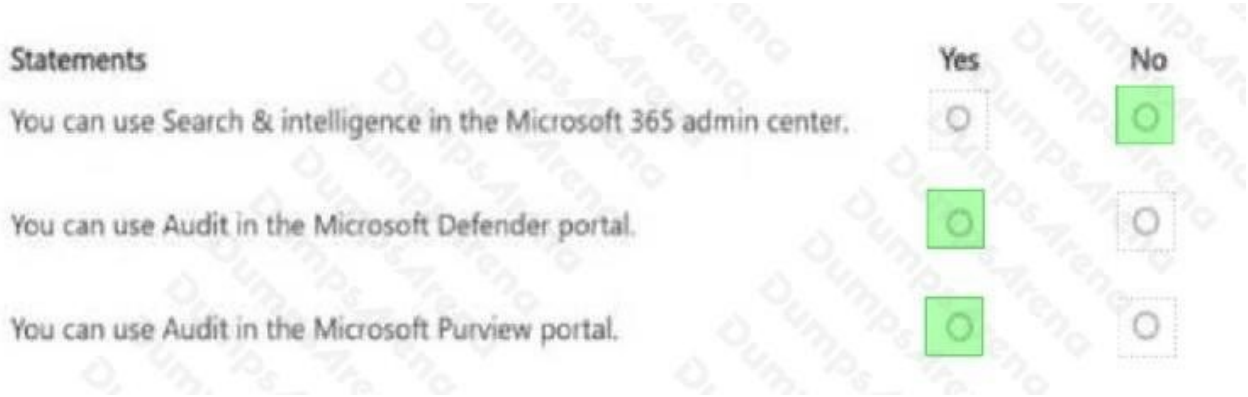
For the third statement, site owners have the ability to manage permissions, including the Owners group membership. That means an owner can remove another owner (with the practical caveat that the site must retain at least one owner so it remains administrable). Microsoft’s documentation on managing owners/members supports that owners can add or remove people from these roles: Change a group owner or member in Microsoft 365. Putting it together, all three statements are true, so you select Yes for each row.

QUESTION NO: 4 - (HOTSPOT)

HOTSPOT

You want to view the administrative actions taken by a service administrator in Microsoft 365. 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:



Explanation:

To view administrative actions taken by a service administrator in Microsoft 365, you're really looking for where you can search the *unified audit log*. Microsoft positions this capability under Microsoft Purview Audit, which records and lets you search activities performed by users and admins across Microsoft 365 services. That's why the Microsoft Purview portal is a correct place to go: the Audit solution in Purview is the primary, documented interface for searching audit records and investigating admin activity.

Microsoft also exposes an Audit experience in the Microsoft Defender portal. Even though Defender is primarily a security portal, its Audit page can be used to search the same unified audit log data for user and admin actions. In other words, using Audit in the Defender portal is also a valid way to review administrative actions, because it's effectively another entry point to the same audit log search capability.

On the other hand, "Search & intelligence" in the Microsoft 365 admin center is not the standard Microsoft feature used to investigate administrator actions through the unified audit log. While the admin center has search features for finding settings, users, and content, Microsoft's documented approach for reviewing admin actions is to use Purview Audit (and the equivalent audit search surfaced elsewhere, like Defender). Therefore, the first statement should be marked No, and the second and third statements should be marked Yes.

References: Microsoft Purview Audit (overview), Search the audit log in Microsoft Purview, Audit in Microsoft Defender (unified audit log search).

QUESTION NO: 5

You plan to create an agent in the Microsoft 365 Copilot app to solve a business issue. What are two reasons to create the agent? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. You need to group related chats into a Copilot notebook.

B. You need to use a custom AI model.

C. You need to use a custom set of instructions that differ from those of the chat experience.

D. You need to reason over a specific website.

ANSWER: C D

Explanation:

In the Microsoft 365 Copilot app, you create an agent when you need Copilot behavior that's more tailored than the default chat experience. A key reason is to apply a **custom set of instructions** (prompting/behavioral guidance) so the agent consistently responds in a way that matches a specific business scenario (for example, a helpdesk triage agent or a policy Q&A agent). That aligns with option C.

A second major reason is to ground the agent on **specific knowledge sources** so it can reason over targeted content rather than only relying on general context. Agent Builder supports adding knowledge such as SharePoint sites/files and public websites, which directly supports option D (reasoning over a specific website).

Option A is incorrect because "grouping related chats into a notebook" is a Copilot organizational feature, not a primary motivation for building an agent. Option B is incorrect in this context because using a *custom AI model* is not a standard capability you select when creating an agent in the Microsoft 365 Copilot app's Agent Builder; custom model selection is typically associated with other build experiences (for example, Copilot Studio/Azure AI) rather than in-app agent creation.

References: https://learn.microsoft.com/en-us/microsoft-365-copilot/extensibility/agents-overview, https://learn.microsoft.com/en-us/microsoft-365-copilot/extensibility/agent-builder

QUESTION NO: 6

Your organization has a Microsoft 365 subscription. All users are assigned a Microsoft 365 Copilot license.

You need to prevent the users from generating images by using Copilot. What should you use?

A. the Microsoft Defender portal

B. the Microsoft Purview portal

C. the Microsoft 365 admin center

D. the Microsoft Entra admin center

ANSWER: C

Explanation:

Correct answer: **C. the Microsoft 365 admin center**. Microsoft provides an admin control specifically for Copilot image generation in the Microsoft 365 admin center. In the Copilot settings, admins can manage whether users are allowed to generate images. When image generation is disabled, Copilot won't create new images and will instead return alternatives such as stock/brand images, which directly meets the requirement to prevent users from generating images via Copilot.

The other options don't match where Microsoft documents this particular control. The Microsoft Defender portal focuses on security operations (threat protection, incidents, etc.) and isn't where Copilot feature toggles like image generation are managed. The Microsoft Purview portal is for compliance, information protection, and governance; while Purview can control data and content policies, it isn't the documented place to toggle Copilot's image generation capability. The Microsoft Entra admin center is primarily for identity and access management (users, groups, app access, conditional access), not for configuring Copilot feature settings like image generation.

References: Microsoft Learn: Manage Microsoft 365 Copilot (Copilot settings), Microsoft Learn: Manage Copilot in the Microsoft 365 admin center.

QUESTION NO: 7

You need to create a Microsoft 365 Copilot agent that can create charts and visualizations based on a Microsoft Excel workbook. What should you configure for the agent?

A. the Scrum Assistant template

B. the Customer Insights Assistant template

C. the code interpreter capability

D. the image generator capability

ANSWER: C

Explanation:

Correct answer: **C. the code interpreter capability**.

To create charts and visualizations from an Excel workbook, the agent needs a capability that can actually *analyze tabular data* and *generate visual outputs* programmatically. In Microsoft 365 Copilot declarative agents, the **code interpreter** capability is designed for exactly this: it can generate and run code (for example, Python) to perform data analysis and produce charts/visualizations from files such as spreadsheets. This aligns directly with the requirement to work from an Excel workbook and output charts.

Option D (image generator) is focused on creating images from prompts (creative generation), not on reading workbook data and computing chart outputs from that data. Options A and B are templates (prebuilt agent patterns) and don't represent the specific technical capability required to parse/analyze Excel data and render visualizations.

References: Microsoft Learn: Agents overview (Copilot extensibility), Microsoft Learn: Declarative agents.

QUESTION NO: 8

Your organization has a Microsoft 365 subscription.

You need to review the impact of a recent phishing incident that targeted email users. What should you use?

A. the Microsoft Defender portal

B. the Microsoft 365 admin center

C. the Microsoft Entra admin center

D. the Microsoft Exchange admin center

ANSWER: A

Explanation:

Correct answer: **A. the Microsoft Defender portal**.

To review the impact of a phishing incident targeting email users, you use the Microsoft Defender portal (Microsoft Defender XDR), because that's where Microsoft Defender for Office 365 investigation and reporting experiences live. From the Defender portal you can analyze phishing campaigns and messages, see which users were targeted, review detections, and assess impact using tools like Explorer/Threat Explorer, campaign views, and incident investigation. These capabilities are designed specifically for security operations workflows (investigate, hunt, remediate) and provide the most direct visibility into email-borne threats and their scope.

Why the others are wrong: The Microsoft 365 admin center is primarily for tenant/user/service administration and high-level reports, not deep phishing investigation. The Microsoft Entra admin center focuses on identity (users, apps, conditional access) rather than email threat analytics. The Exchange admin center is for Exchange configuration (mail flow, protection policies configuration in some cases), but Microsoft's current guidance for investigating phishing and email threats centers on the Defender portal's security investigation tools.

References: Threat Explorer in Microsoft Defender for Office 365, Incidents in Microsoft Defender XDR

QUESTION NO: 9

Your organization has a Microsoft 365 subscription.

You need to evaluate your organization's Identity Secure Score.

Which two factors affect the score? Each correct answer presents a complete the solution. NOTE: Each correct selection is worth one point.

A. the SharePoint site permissions

B. the number of global administrators

C. passwords that are never expired

D. the location of the users

ANSWER: B C

Explanation:

Identity Secure Score (in Microsoft Entra) is calculated from identity-focused security recommendations and how well your tenant aligns to them. Two common recommendations that directly impact the score are (1) ensuring you have appropriate administrative coverage (for example, having more than one Global Administrator so you're not locked out) and (2) strengthening authentication hygiene, including password policy guidance such as avoiding configurations that weaken security posture. Therefore, the number of Global Administrators and whether passwords are configured to never expire are factors that can affect the Identity Secure Score.

SharePoint site permissions (Option A) are part of SharePoint/Microsoft 365 content governance and do not feed into Entra's Identity Secure Score, which is scoped to identity controls (accounts, roles, authentication methods, Conditional Access, etc.). User location (Option D) can be used in Conditional Access policies, but "the location of the users" itself is not a scored factor; what's scored is whether you've implemented identity controls/recommendations (for example, location-based Conditional Access), not the geographic attribute alone.

References: Microsoft Entra Identity Secure Score, Microsoft Entra built-in roles (including Global Administrator).

QUESTION NO: 10

Your organization has a Microsoft 365 subscription.

You need to evaluate your organization s Identity Secure Score.

Which two factors affect the score? Each correct answer presents a complete the solution. NOTE: Each correct selection is worth one point.

A. the number of global administrators

B. the SharePoint site permissions

C. the location of the users

D. passwords that are never expired

ANSWER: A D

Explanation:

Microsoft Entra Identity Secure Score is driven by how well your tenant aligns to Microsoft's identity security recommendations. In practice, the score increases as you implement recommended identity controls and decreases (or stays lower) when those controls are missing. Two examples of recommendations that directly influence the score are ensuring you have appropriate administrative role coverage (for example, not relying on a single Global Administrator) and improving credential hygiene (for example, avoiding password policies that weaken security posture).

Therefore, **A** is correct because Identity Secure Score includes recommendations related to privileged role assignments and administrative governance, and the presence/coverage of Global Administrators is part of that identity posture. **D** is also correct because password policy settings (including whether passwords expire or never expire) are part of identity configuration and are evaluated through identity security recommendations that contribute to the score.

B is incorrect because SharePoint site permissions are workload/resource authorization settings and are not part of Entra Identity Secure Score's identity-focused recommendations. **C** is incorrect because while user location can be used in Conditional Access policies, "the location of the users" itself isn't a direct scoring factor; the score tracks whether recommended controls (like Conditional Access) are configured, not where users physically reside.

References: Microsoft Learn: Identity Secure Score, Microsoft Learn: Security defaults (identity security posture)