PassQueen
a.k.a dumpsqueen.com

Microsoft 365 Copilot and Agent Administration Fundamentals

Microsoft AB-900

Version Demo

Total Demo Questions: 20

Total Premium Questions: 202

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Describe Microsoft 365 Copilot and agents	24
Topic 2, Describe security and compliance for Microsoft 365 Copilot and agents	106
Topic 3, Describe administration of Microsoft 365 Copilot and agents	69
Topic 4, Mix Questions	3
Total	202

QUESTION NO: 1

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:

The Microsoft Defender portal is the appropriate place to review the impact of a phishing incident targeting email users. It provides the unified Microsoft Defender XDR security-operations experience, where security teams can investigate incidents, alerts, affected users, mailboxes, devices, and related evidence across Microsoft 365 services. For email-based phishing, Microsoft Defender for Office 365 capabilities within the portal, including Explorer (also called Threat Explorer), enable analysts to search for malicious or suspicious messages and assess delivery status, recipients, detections, URLs, attachments, and user actions. This supports determining the incident's scope and identifying the users and assets that may require remediation. The portal's incident experience also correlates related alerts and entities into a consolidated investigation, helping responders understand the phishing campaign's impact and take follow-up response actions from one security-focused interface. These investigation capabilities are specifically designed for analyzing email threats and their organizational impact. For details, see Threat Explorer in Microsoft Defender for Office 365 and Incidents in Microsoft Defender XDR.

QUESTION NO: 2

Your organization wants to use Microsoft 365 Copilot agents responsibly.

Which two practices support responsible deployment of agents? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Test the agent before broad deployment.

B. Provide clear user guidance.

C. Allow the agent to bypass user permissions.

D. Remove human review from all business decisions.

ANSWER: A B

Explanation:

Testing an agent before broad deployment is correct because testing helps validate that the agent follows its intended instructions, provides relevant responses, and behaves appropriately with its configured knowledge and actions. Testing also helps identify issues that require refinement before users rely on the agent.

Providing clear user guidance is also correct because users should understand the agent's intended purpose, limitations, and the need to review outputs before using them in business decisions. Human oversight remains important when an agent assists with work involving organizational data.

Microsoft's responsible AI principles include reliability and safety, transparency, privacy and security, and accountability. See Microsoft Responsible AI and Microsoft 365 Copilot agents overview.

QUESTION NO: 3 - (SIMULATION)

You open the Microsoft Entra admin center as shown in the following exhibit.

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

ANSWER: See the explanation for the answer

Explanation:

Answer: Require multifactor authentication for administrative roles.

This recommendation has **0/10 Secure Score points**. Completing it can therefore increase the Identity Secure Score by **10 points**, which is greater than the available improvements for the other displayed recommendations:

Use least privileged administrative roles: **1/1** (no points remaining)
Do not expire passwords: **8/8** (no points remaining)
Enable policy to block legacy authentication: **0.73/8** (up to 7.27 points remaining)
Require multifactor authentication for administrative roles: **0/10** (10 points remaining)

QUESTION NO: 4

Your company has a Microsoft SharePoint site named Site1. Site1 contains all the policies of the company s HR department. The policies are saved as Microsoft Word documents.

All users have read access to Site1.

The HR department manager reports that user requests about the policies are NOT being addressed in a timely manner, especially around major holidays.

You need to recommend a solution to enable the users to find the HR department policies. The solution must provide the users with a list of common queries and ensure that responses are grounded only in Site1.

What should you include in the recommendation?

A. the personal assistant in Copilot in Word

B. a Microsoft 365 Copilot notebook

C. a custom Microsoft 365 Copilot agent

D. the Researcher agent in Microsoft 365 Copilot

ANSWER: C

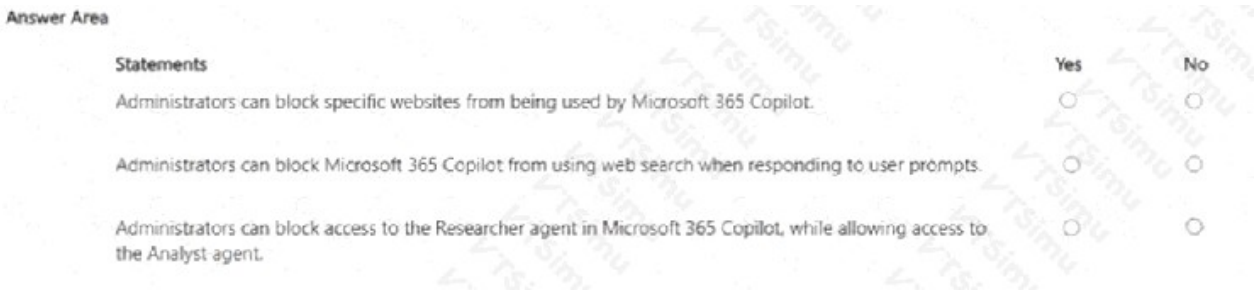
Explanation:

A custom Microsoft 365 Copilot agent is the appropriate recommendation because it can be tailored to a focused business scenario, such as answering questions about HR policies. The agent can use the SharePoint content in Site1 as its knowledge source, allowing answers to be based on the approved policy documents that users already have permission to read. This creates a self-service experience for commonly requested information, including questions that may increase around holidays, while maintaining the intended scope of HR policy content.

An agent can also include suggested prompts, commonly called conversation starters. These present users with a list of useful, common queries when they open the agent—for example, prompts related to holiday schedules, leave, or benefits—so users do not need to formulate every question from scratch. Configuring Site1 as the agent's knowledge source and limiting its grounding to that source supports the requirement that responses come only from the designated HR policy repository. Microsoft describes Microsoft 365 Copilot agents as customized experiences that can be grounded in selected organizational knowledge, and documents how SharePoint content can be used as a knowledge source for agents. See Agents for Microsoft 365 Copilot overview and Use SharePoint and OneDrive for generative answers.

QUESTION NO: 5 - (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:

Microsoft 365 Copilot administration provides a tenant-level control for web grounding rather than a standard control for selecting individual public websites that Copilot may use in ordinary responses. The relevant setting is **Allow web search in Copilot**. An administrator can turn that setting off to prevent Microsoft 365 Copilot and Copilot Chat from using web search when they respond to user prompts. This makes the statement about blocking Microsoft 365 Copilot from using web search true. Microsoft documents this setting and its administrative configuration in its Manage web search in Microsoft 365 Copilot guidance.

Microsoft also supports governance of individual Microsoft-provided agents. In the Microsoft 365 admin center, an administrator can manage availability of agents and use the Block action for an agent. Researcher and Analyst are independently governed agents, so blocking Researcher does not require blocking Analyst as well. This makes the statement about blocking access to the Researcher agent while continuing to allow access to the Analyst agent true. Microsoft describes agent controls, including the ability to block agents, in Manage agents in the Microsoft 365 admin center.

Consequently, the correct hotspot pattern is No for the specific-website statement, Yes for the web-search statement, and Yes for the Researcher-only access statement. The provided answer image places the selections in exactly those locations.

QUESTION NO: 6

You are configuring a Microsoft Purview sensitivity label for confidential project documents.

Which two protections can the label apply to files? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Encryption

B. Content markings

C. Mailbox quota increases

D. Microsoft Entra role assignments

ANSWER: A B

Explanation:

Encryption is correct because a sensitivity label can apply encryption settings to supported files and emails. Encryption can define which users can access the protected content and what rights they have, such as viewing or editing.

Content markings are also correct because sensitivity labels can add visual markings, such as headers, footers, and watermarks, to supported documents. These markings help users identify the sensitivity of content while the label's configured protection remains associated with the file. See Microsoft Purview sensitivity labels.

QUESTION NO: 7

Your organization needs to use a retention policy for SharePoint and OneDrive content.

Which two outcomes can a retention policy enforce? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Retain content for a specified period.

B. Delete content after the retention period.

C. Require multifactor authentication for site access.

D. Assign Microsoft 365 Copilot licenses.

ANSWER: A B

Explanation:

Retaining content for a specified period is correct because a retention policy can preserve in-scope content for a configured duration to meet business, legal, or regulatory requirements. Depending on the configuration, content can be retained even when users attempt to delete it.

Deleting content after the retention period is also correct because a retention policy can be configured to delete content when the retention duration ends. This enables organizations to manage the lifecycle of data according to their records-management requirements. See Learn about retention in Microsoft Purview.

QUESTION NO: 8

Your organization creates a Microsoft Purview eDiscovery case for a legal investigation.

Which two tasks can you perform in the case? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create holds for relevant content

B. Search and collect in-scope content

C. Publish sensitivity labels to users

D. Create Conditional Access policies

ANSWER: A B

Explanation:

You can create holds in an eDiscovery case to preserve relevant content for the legal matter. Holds help ensure that in-scope information is retained even if a user attempts to delete or modify it.

You can search and collect content in an eDiscovery case. This enables authorized legal and compliance personnel to identify potentially relevant content from supported Microsoft 365 locations and prepare it for review.

Publishing sensitivity labels and creating Conditional Access policies are managed through other Microsoft Purview and Microsoft Entra administration experiences. See Microsoft Purview eDiscovery solutions and Create an eDiscovery case.

QUESTION NO: 9 - (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:

Answer:

Answer:

Explanation:

To use Microsoft 365 Copilot Chat to reason over web data, you need a Microsoft 365 Copilot license. **Answer: No**
To use the Researcher agent in Microsoft 365 Copilot, you need a Microsoft 365 Copilot license. **Answer: Yes**To add an agent in the Microsoft 365 Copilot app, you need a Microsoft 365 Copilot license. **Answer: No**The correct selections are **No, Yes, No** . Microsoft documents that **Microsoft 365 Copilot Chat** is available at no additional cost for eligible Entra account users with qualifying Microsoft 365 licenses, and that it includes **secure AI chat grounded in the web** . That means a separate Microsoft 365 Copilot add-on license is **not** required just to use Copilot Chat over web data.Statement 2 is **Yes** because Microsoft states that **Researcher** is part of the core default experience for **Microsoft 365 Copilot licensed users** . In other words, access to the Researcher agent requires the Microsoft 365 Copilot license.Statement 3 is **No** because Microsoft documents that users can **access agents and create them in the Microsoft 365 Copilot app** through Copilot Chat, and Microsoft 365 service descriptions state that **web-grounded agents** are available at no extra cost for commercial users with a qualifying Microsoft 365 license. A Copilot add-on license is required for certain advanced capabilities, but not simply to add an agent in the app in general.

Explanation:

Microsoft 365 Copilot Chat can be used with web grounding by eligible users who have a qualifying Microsoft 365 subscription and sign in with a work or school account. This Copilot Chat experience is included at no additional cost for eligible commercial customers; therefore, a separate Microsoft 365 Copilot add-on license is not required merely to ask questions and reason over publicly available web information. Microsoft describes this as secure AI chat with web grounding, with enterprise data protection for eligible users. The applicable selection for the statement about reasoning over web data in Copilot Chat is No.

Researcher is a Copilot agent intended for deeper, multi-step research and synthesis. It is included in the Microsoft 365 Copilot experience for users assigned a Microsoft 365 Copilot license. That license gives the user access to the work-grounded Copilot capabilities and agents provided as part of the licensed experience, including Researcher. Consequently, the applicable selection for the statement about using the Researcher agent is Yes.

Adding an agent in the Microsoft 365 Copilot app does not, by itself, universally require the Microsoft 365 Copilot add-on license. Eligible users can discover and use certain agents through Copilot Chat, including web-grounded agent experiences available with qualifying Microsoft 365 licenses. Licensing requirements can differ for specific agents, premium capabilities, organizational data access, or custom agent features, but the general action of adding an agent in the app is not restricted

only to Microsoft 365 Copilot license holders. Therefore, the applicable selection for the statement about adding an agent is No. Microsoft's licensing overview is available at Microsoft 365 Copilot Chat, and Microsoft documents agent availability at Microsoft 365 Copilot agents.

QUESTION NO: 10

Copilot monthly licensing differs from pay-as-you-go by:

A. Charging per seat rather than per usage event

B. Requiring a local server

C. Bundling Teams phone features

D. Removing all limits on API usage

ANSWER: A

Explanation:

Charging per seat rather than per usage event is correct because monthly licensing for Microsoft 365 Copilot is a subscription-based licensing model. An organization obtains licenses and assigns them to individual users, with billing based on the number of licensed users for the subscription term. This provides a predictable cost structure and gives each licensed user access to the Copilot capabilities included with their license. Microsoft describes Microsoft 365 Copilot as an add-on license that is assigned to users through standard Microsoft 365 licensing administration. In contrast, pay-as-you-go billing is consumption based: costs are calculated from measured usage rather than from a fixed allocation of user licenses. This distinction matters when an organization chooses how to provide Copilot capabilities, because seat-based licensing is centered on granting named users ongoing access, while consumption billing is centered on the volume of service used. The licensing approach therefore affects both cost predictability and how access is provisioned. Microsoft's licensing guidance for Microsoft 365 Copilot and its documentation on Copilot Studio billing describe these subscription and consumption-based models. See Microsoft 365 Copilot licensing and Copilot Studio billing and licensing.

QUESTION NO: 11

Your organization needs to detect potentially inappropriate or noncompliant employee communications.

Which two communication types can Microsoft Purview Communication Compliance monitor? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Exchange Online email messages

B. Microsoft Teams chat and channel messages

C. SharePoint document libraries

D. Microsoft Entra sign-in logs

ANSWER: A B

Explanation:

Microsoft Purview Communication Compliance can monitor Exchange Online email communications. Policies can identify communications that match configured conditions and provide reviewers with workflows to investigate potentially risky messages.

Communication Compliance can also monitor Microsoft Teams chats and channel messages. This helps organizations address risks such as harassment, threats, adult content, and the sharing of sensitive information in supported communication channels.

SharePoint documents and Microsoft Entra sign-in logs are not communication types monitored by Communication Compliance policies. See Learn about Microsoft Purview Communication Compliance.

QUESTION NO: 12

You plan to create an agent by using Agent Builder in the Microsoft 365 Copilot app.

Which two configurations can you define for the agent? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Custom instructions

B. A SharePoint site as a knowledge source

C. A Conditional Access policy

D. A Microsoft 365 product license assignment

ANSWER: A B

Explanation:

Custom instructions can be configured for an agent. Instructions define the agent's purpose, expected behavior, tone, boundaries, and the way that it should respond to users. This allows an organization to create an experience that is focused on a particular business scenario.

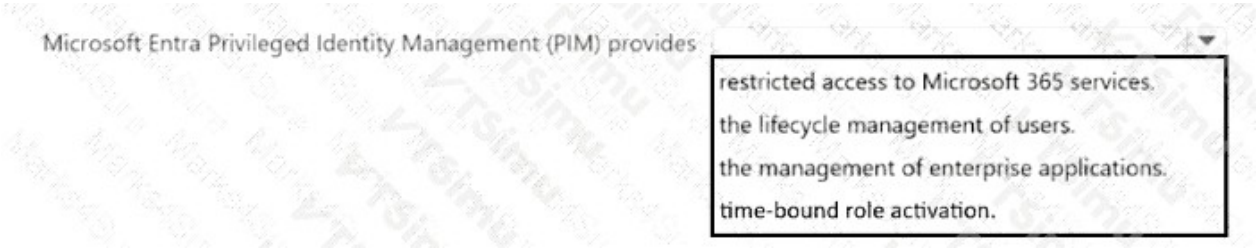
A SharePoint site can also be configured as an agent knowledge source. The agent can use the selected site to ground responses in relevant organizational content, while continuing to respect the permissions of the user who interacts with the agent.

Conditional Access policies are configured in Microsoft Entra ID, and licenses are assigned through Microsoft 365 administration experiences. Neither is an Agent Builder configuration. See Build agents with Agent Builder and Agents for Microsoft 365 Copilot overview.

QUESTION NO: 13 - (SIMULATION)

Select the answer that correctly completes the sentence.

Microsoft Entra Privileged Identity Management (PIM) provides **time-bound role activation** .



ANSWER: See the explanation for the answer

Explanation:

Select **time-bound role activation**.

Microsoft Entra Privileged Identity Management (PIM) enables just-in-time privileged access: users can be eligible for a role and activate it only when needed, for a configured limited duration. The role assignment expires after that activation period.

QUESTION NO: 14

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:

Creating an agent is appropriate when the business scenario needs behavior and knowledge that are intentionally scoped beyond the general Microsoft 365 Copilot chat experience. “You need to use a custom set of instructions that differ from those of the chat experience.” is correct because an agent can be given dedicated instructions that establish its purpose, expected behavior, tone, response format, and boundaries. Those instructions are applied whenever users interact with that agent, helping it deliver a consistent experience for a specialized business process, such as policy guidance, onboarding support, or help-desk triage.

“You need to reason over a specific website.” is also correct because an agent can be configured with selected knowledge sources, including public websites where supported. This grounds the agent’s responses in content relevant to the defined scenario rather than relying only on the broad context available to standard chat. Combining focused instructions with curated knowledge enables an organization to create a purpose-built experience that helps users retrieve and apply information from an authoritative site. Microsoft describes agents as customized Copilot experiences that use instructions, knowledge, and actions to carry out defined tasks. See Microsoft 365 Copilot agents overview and Create agents with Agent Builder.

QUESTION NO: 15

Insider Risk Management helps organizations:

A. Create Teams channels

B. Detect risky user behaviors and potential data leakage

C. Disable all external emails

D. Encrypt Azure SQL databases

ANSWER: B

Explanation:

Microsoft Purview Insider Risk Management helps organizations detect, investigate, and act on potentially risky user activities that could result in security, privacy, or compliance incidents. Therefore, **Detect risky user behaviors and potential data leakage** is correct. The solution correlates relevant signals from Microsoft 365 workloads and endpoints, including activities involving sensitive data, file movement, downloads, sharing, and communications. It uses policies and risk indicators to identify patterns associated with scenarios such as data leakage, security policy violations, and risks involving departing employees. Alerts are prioritized so that authorized analysts can investigate significant activity and take appropriate action before an issue becomes a material incident. Insider Risk Management also incorporates privacy protections, including role-based access controls and pseudonymization, helping organizations manage internal risk while limiting exposure of user information to only those who require access for an investigation. These capabilities make it a governance and risk-management tool for protecting organizational data from accidental or malicious insider actions. Microsoft documents that Insider Risk Management is intended to help identify, investigate, and remediate internal risks before they adversely affect an organization. See Microsoft Purview Insider Risk Management and Insider Risk Management policies.

QUESTION NO: 16

Your company is piloting the use of Microsoft 365 Copilot and has purchased 100 Microsoft 365 Copilot licenses.

You need to view detailed reports about Copilot usage in Microsoft Teams, such as meeting hours summarized by Copilot and meeting actions taken by using Copilot.

What should you use?

A. the Microsoft 365 Apps usage report in the Microsoft 365 admin center

B. the Microsoft 365 Copilot readiness report in the Microsoft 365 admin center

C. the Microsoft 365 Copilot dashboard in Microsoft Viva Insights

D. the Microsoft 365 Copilot usage report in the Microsoft 365 admin center

ANSWER: D

Explanation:

The Microsoft 365 Copilot usage report in the Microsoft 365 admin center is the appropriate reporting tool because it provides tenant-level usage data for Microsoft 365 Copilot across supported apps, including Microsoft Teams. For Teams, the report includes the specific meeting measures required in the scenario: meeting hours summarized by Copilot and meeting actions taken using Copilot. These metrics let an administrator assess how licensed users are adopting Copilot's meeting capabilities during a pilot, rather than merely confirming that licenses were assigned or that users are eligible for Copilot.

The report is available in the Microsoft 365 admin center under **Reports** and **Usage**. It presents aggregate trends and can help organizations understand usage over a selected reporting period, which supports pilot evaluation, adoption tracking, and decisions about broader deployment. Microsoft documents the available measures and report access in its Microsoft 365 Copilot usage report guidance. For the broader set of Microsoft 365 usage-reporting capabilities and administrative access requirements, see Activity reports in the Microsoft 365 admin center.

QUESTION NO: 17

Your organization plans to deploy Microsoft 365 Copilot.

You need to reduce the risk that Copilot surfaces content that is accessible through excessive permissions.

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

NOTE: Each correct selection is worth one point.

A. Review SharePoint and OneDrive permissions.

B. Apply least-privilege access.

C. Assign Global Administrator to all Copilot users.

D. Disable multifactor authentication for licensed users.

ANSWER: A B

Explanation:

Reviewing SharePoint and OneDrive permissions is correct because Microsoft 365 Copilot respects the existing permissions of the signed-in user. Content that is overshared can be available to users through Copilot if those users already have access to the content. Reviewing direct permissions, group membership, and sharing links helps identify and remediate unnecessary access.

Applying least-privilege access is also correct because it ensures users receive only the access needed for their roles. This reduces exposure in Microsoft 365 generally and limits the organizational data that can be used to ground a user's Copilot responses. See Data, Privacy, and Security for Microsoft 365 Copilot and Zero Trust identity guidance.

QUESTION NO: 18

Copilot license assignment is done through:

A. Teams admin center

B. Microsoft 365 admin center

C. Azure Firewall

D. Local Group Policy

ANSWER: B

Explanation:

Microsoft 365 admin center is correct because Microsoft 365 Copilot is licensed as a Microsoft 365 service, and administrators assign its licenses to users through the central Microsoft 365 administration portal. In the Microsoft 365 admin center, an administrator can assign licenses individually from the active user's license and apps settings, assign licenses to multiple users in bulk, or use group-based licensing where available. This ensures that the intended users receive the Microsoft 365 Copilot service plan and can access Copilot capabilities in the Microsoft 365 apps and experiences for which they are eligible. The same portal also provides the subscription and billing context needed to confirm that Copilot licenses have been purchased and are available for assignment. Microsoft's deployment guidance specifically identifies the Microsoft 365 admin center as the place to assign Microsoft 365 Copilot licenses during setup. Administrators should also ensure users have the required base Microsoft 365 license and meet the applicable service prerequisites before assigning Copilot. For details, see Microsoft 365 Copilot setup and Assign licenses to users in the Microsoft 365 admin center.

QUESTION NO: 19

Your organization has a Microsoft 365 subscription that uses Microsoft Entra ID. You have a custom web app named App1.

Users automatically authenticate to App1 by using their Microsoft Entra credentials, without manually entering their credentials.

What is this an example of?

A. multifactor authentication (MFA)

B. password synchronization

C. pass-through authentication

D. single sign-on (SSO)

ANSWER: D

Explanation:

Single sign-on (SSO) is the capability that enables a user to authenticate once with Microsoft Entra ID and then access an application without being prompted to enter credentials again. In this case, App1 is configured to trust Microsoft Entra ID as its identity provider. When a user has an existing Microsoft Entra session, the application can use that session and the associated identity tokens or assertions to establish access automatically. This creates a smoother user experience because the user does not need a separate username and password for App1 or a new interactive sign-in each time they open it. For a custom web application, SSO is commonly implemented by registering the application in Microsoft Entra ID and using standards such as OpenID Connect or OAuth 2.0 to obtain and validate tokens. Microsoft Entra ID provides SSO across cloud applications and custom applications that are integrated with the tenant, while still allowing applicable Conditional

Access policies to be evaluated during authentication. See Microsoft Entra single sign-on overview and OpenID Connect on the Microsoft identity platform.

QUESTION NO: 20

Your organization has a Microsoft 365 subscription.

Your company recently purchased Microsoft 365 Copilot licenses for some users.

You need to identify how many unlicensed users have used Copilot in Microsoft Teams.

Which usage report should you use in the Microsoft 365 admin center?

A. Microsoft 365 Copilot Chat

B. Microsoft 365 Copilot Search

C. Microsoft 365 Copilot

D. Microsoft 365 Apps

ANSWER: A

Explanation:

Microsoft 365 Copilot Chat is the appropriate usage report because it provides adoption and activity information for Copilot Chat, including use by unlicensed users. In the Microsoft 365 admin center, this report helps administrators understand how users interact with Copilot Chat across its available entry points and experiences. Microsoft Teams is one of the supported places from which users can access Copilot Chat, so the report is suitable for determining the number of unlicensed users who used Copilot through Teams.

This distinction matters because Copilot Chat can be available to eligible Microsoft 365 users without an assigned Microsoft 365 Copilot license, while the licensed Microsoft 365 Copilot experience is reported separately. The Copilot Chat report includes metrics that distinguish licensed and unlicensed users, allowing the organization to identify unlicensed adoption and use that may inform license assignment, rollout planning, and governance decisions. Administrators can access the report from the Usage area of the Microsoft 365 admin center and use its filters and user-level details to examine relevant activity. Microsoft documents the available Copilot usage reports and the Copilot Chat reporting metrics in the Microsoft 365 Copilot usage report documentation and the Microsoft 365 Copilot Chat usage report documentation.