

AB-900

PRACTICE QUESTION BANK

Microsoft 365 Copilot and Agent Administration Fundamentals

125 original multiple-choice questions | Five mixed practice exams | Complete answer key

5

PRACTICE EXAMS

125

QUESTIONS

1

COMPLETE KEY

Independent study resource - not endorsed by Microsoft

Version 1.0 | July 2026

IMPORTANT EXAM CONTENT DISCLAIMER

Original practice material

The questions in this guide are independently written from publicly documented Microsoft learning objectives.

They are not copied, recalled, reconstructed or adapted from the live AB-900 exam.

The exact questions, choices, scenarios and wording from a live certification exam cannot be shared.

This question bank was compiled from a series of study sessions and lightly standardised for consistent wording and formatting. Some concepts intentionally appear more than once in different scenarios because repetition helps reinforce the product hierarchy and the distinctions that commonly cause confusion.

Exam objectives and Microsoft product capabilities can change. Check the current official AB-900 study guide before using this resource as part of an exam preparation plan.

Official study guide: [Microsoft Learn - Study guide for Exam AB-900](#)

Candidate agreement: [Microsoft Certification Exam Candidate Agreement](#)

Official practice assessment information: [Practice Assessments for Microsoft Certifications](#)

HOW TO USE THIS BOOK

1. Sit each exam without notes

Each exam contains 25 mixed questions. Mark any question you are unsure about, even when you select the correct answer.

2. Review the explanation, not only the letter

The answer key includes a concise rationale so you can identify why the correct product or feature fits the scenario.

3. Track repeated mistakes

Create a short revision list for distinctions such as SITs vs labels vs DLP, Audit vs eDiscovery, and Intune vs Conditional Access.

4. Verify against Microsoft Learn

Use the official study guide and product documentation as the final authority, especially after exam updates.

CONTENTS

SECTION	DESCRIPTION
Memory framework	The product hierarchy and key exam verbs
Answer sheet	A single sheet for all five exams
Practice Exam 1	Questions 1-25
Practice Exam 2	Questions 1-25
Practice Exam 3	Questions 1-25
Practice Exam 4	Questions 1-25
Practice Exam 5	Questions 1-25
Complete answer key	Answers and concise explanations
Official references	Microsoft Learn sources

THE AB-900 MEMORY FRAMEWORK

Start by identifying the type of problem described in the question. Then choose the Microsoft product or feature that owns that problem.

PROBLEM AREA	PRIMARY MICROSOFT PRODUCT
PEOPLE	Microsoft Entra ID
DEVICES	Microsoft Intune
DATA	Microsoft Purview
ATTACKS	Microsoft Defender
AI	Microsoft 365 Copilot
SPECIFIC AI ASSISTANT	Agent

PURVIEW: DETECT, PROTECT, PREVENT

DETECT	PROTECT	PREVENT
Sensitive Information Types (SITs)	Sensitivity labels	Data Loss Prevention (DLP)

OTHER HIGH-VALUE VERBS

QUESTION CLUE	THINK ABOUT
ACTIONS	Audit
LEGAL	eDiscovery
KEEP	Retention
EMPLOYEE RISK	Insider Risk Management
MESSAGES	Communication Compliance
AI DATA RISK	DSPM for AI
REQUIRE MFA	Conditional Access
DETERMINE COMPLIANCE	Microsoft Intune
REQUIRE COMPLIANT DEVICE	Conditional Access

Copilot permission rule

Microsoft 365 Copilot respects the user's existing permissions.
Copilot can make already accessible information easier to discover, but it does not automatically grant access to protected content.

ANSWER SHEET

Write A, B, C or D in each cell. Mark uncertain answers with a question mark so you remember to review them even if your guess is correct.

Q	EXAM 1	EXAM 2	EXAM 3	EXAM 4	EXAM 5
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					
25					

PRACTICE EXAM 1

25 mixed questions | Select the single best answer for each question

1. An organisation wants users to complete MFA whenever Microsoft Entra detects a high-risk sign-in.
 - A. Data Loss Prevention
 - B. Conditional Access
 - C. Sensitivity labels
 - D. Microsoft Defender XDR

2. An administrator needs to determine which user deleted a confidential file from a SharePoint site.
 - A. Audit
 - B. eDiscovery
 - C. Retention
 - D. Communication Compliance

3. A company needs to identify documents containing credit card numbers. Which feature provides the underlying method of recognising this information?
 - A. Retention labels
 - B. Sensitive Information Types
 - C. Conditional Access
 - D. Privileged Identity Management

4. Finance documents must be encrypted, and users outside the Finance department must not be able to open them.
 - A. Data Loss Prevention
 - B. Sensitivity labels
 - C. Microsoft Defender XDR
 - D. Communication Compliance

5. An organisation wants to block employees from emailing documents containing tax file numbers to external recipients.
 - A. Data Loss Prevention
 - B. Audit
 - C. Single sign-on
 - D. Privileged Identity Management

6. A business must retain employee emails for seven years before they can be deleted.
 - A. Communication Compliance
 - B. Data Lifecycle Management
 - C. Conditional Access
 - D. Defender XDR

7. A user receives information from a SharePoint document in a Microsoft 365 Copilot response. Why was Copilot able to access the document?
 - A. Copilot automatically receives access to every SharePoint site
 - B. The user already had permission to access the document
 - C. Copilot bypassed the SharePoint permission model
 - D. The document was stored in Microsoft Purview

8. A security analyst needs to investigate an incident involving a malicious email, a compromised identity and activity on an endpoint.

- A. Microsoft Defender XDR
- B. Microsoft Purview eDiscovery
- C. Microsoft Intune
- D. Microsoft 365 Copilot Analytics

9. A legal team needs to find emails and SharePoint files relating to a court case.

- A. Identity Secure Score
- B. Microsoft Purview eDiscovery
- C. Conditional Access
- D. Copilot Analytics

10. An administrator wants to identify SharePoint sites where content may be accessible to more users than necessary.

- A. A SharePoint data access governance report
- B. An Exchange message trace
- C. Identity Secure Score
- D. A Microsoft Defender endpoint inventory

11. An organisation wants administrators to activate elevated roles for two hours rather than permanently holding those roles.

- A. Single sign-on
- B. Privileged Identity Management
- C. Data Loss Prevention
- D. Communication Compliance

12. An administrator wants to measure how frequently employees are using Microsoft 365 Copilot.

- A. Copilot Analytics and usage reports
- B. Microsoft Purview eDiscovery
- C. Defender XDR incidents
- D. Conditional Access insights

13. The HR department wants an AI assistant that answers employee questions using approved policy documents stored in SharePoint.

- A. A distribution group
- B. A custom agent
- C. A Conditional Access policy
- D. An Insider Risk Management policy

14. An organisation wants to receive recommendations for improving its compliance posture.

- A. Compliance Manager
- B. Communication Compliance
- C. Privileged Identity Management
- D. Microsoft Defender XDR

15. A security team wants to identify potentially risky employee activities that could indicate intentional or accidental data theft.

- A. Insider Risk Management
- B. Single sign-on
- C. Copilot Analytics
- D. Exchange mail flow rules

16. A company wants to detect threatening or inappropriate language in workplace communications.
- A. Communication Compliance
 - B. Sensitivity labels
 - C. Conditional Access
 - D. Microsoft Defender for Endpoint
17. An administrator needs to discover AI applications being used and evaluate AI-related data risks.
- A. DSPM for AI
 - B. Privileged Identity Management
 - C. Microsoft Defender XDR
 - D. Retention Management
18. Which admin centre is most appropriate for managing mailboxes and distribution groups?
- A. Microsoft Entra admin centre
 - B. Exchange admin centre
 - C. Microsoft Purview portal
 - D. Power Platform admin centre
19. Which admin centre is most appropriate for reviewing SharePoint sites, libraries and site permissions?
- A. Teams admin centre
 - B. SharePoint admin centre
 - C. Microsoft Defender portal
 - D. Exchange admin centre
20. An organisation needs to control which users can access a newly created agent.
- A. Agent user access
 - B. A retention policy
 - C. A Sensitive Information Type
 - D. Identity Secure Score
21. A new employee cannot use Microsoft 365 Copilot even though their account is active. What should an administrator check first?
- A. Whether an appropriate Copilot licence is assigned
 - B. Whether a DLP alert exists
 - C. Whether the user has created an agent
 - D. Whether a retention label is published
22. Which admin centre is most appropriate for managing teams, channels and Teams policies?
- A. Teams admin centre
 - B. Exchange admin centre
 - C. Microsoft Purview portal
 - D. SharePoint admin centre
23. A developer needs to define an application identity, redirect URI and API permissions in Microsoft Entra ID.
- A. Enterprise application
 - B. App registration
 - C. Conditional Access policy
 - D. Distribution group
24. What is the primary purpose of Identity Secure Score?
- A. To measure identity security posture and recommend improvements
 - B. To calculate Copilot usage charges
 - C. To classify documents by sensitivity
 - D. To investigate endpoint malware

25. Which statement best reflects a core Zero Trust principle?

- A. Trust all users on the corporate network
- B. Verify explicitly and use least-privilege access
- C. Allow access until an incident occurs
- D. Give administrators permanent privileges

PRACTICE EXAM 2

25 mixed questions | Select the single best answer for each question

1. Which Microsoft service primarily manages cloud users, groups and authentication?
 - A. Microsoft Entra ID
 - B. Microsoft Intune
 - C. Microsoft Purview
 - D. Microsoft Defender XDR

2. Which Microsoft service evaluates whether a managed device meets an organisation's compliance rules?
 - A. Microsoft Entra ID
 - B. Microsoft Intune
 - C. Microsoft Purview
 - D. Microsoft Defender XDR

3. Payroll files must carry a Confidential classification and remain encrypted after they are downloaded.
 - A. Sensitive Information Types
 - B. Sensitivity labels
 - C. Data Loss Prevention
 - D. Audit

4. Which feature can recognise a sequence that matches a credit card number?
 - A. Sensitive Information Types
 - B. Sensitivity labels
 - C. Retention policies
 - D. Conditional Access

5. A user attempts to share a file containing passport numbers with an external guest. The action must be blocked.
 - A. Audit
 - B. Data Loss Prevention
 - C. eDiscovery
 - D. Privileged Identity Management

6. An administrator needs to know who changed a sensitivity label on a document.
 - A. Audit
 - B. eDiscovery
 - C. Communication Compliance
 - D. Compliance Manager

7. A legal hold must preserve relevant emails while a legal case is active.
 - A. eDiscovery
 - B. Defender XDR
 - C. Conditional Access
 - D. Copilot Analytics

8. Which solution focuses on risky internal user behaviour, such as unusual downloading before resignation?
 - A. Insider Risk Management
 - B. Communication Compliance
 - C. Identity Secure Score
 - D. Microsoft Intune

9. Which solution is designed to detect harassment or threatening language in Teams and Exchange communications?
- A. Communication Compliance
 - B. Data Lifecycle Management
 - C. Defender for Endpoint
 - D. SharePoint Advanced Management
10. Which solution helps discover generative AI usage and assess how sensitive data is exposed to AI applications?
- A. DSPM for AI
 - B. PIM
 - C. SSO
 - D. Exchange message trace
11. An administrator wants to review activities involving labelled or sensitive content, such as label changes and DLP events.
- A. Activity Explorer
 - B. Data Explorer
 - C. Identity Secure Score
 - D. Defender device inventory
12. An administrator wants an overview of where sensitive information exists across Microsoft 365.
- A. Data Explorer
 - B. Activity Explorer
 - C. Conditional Access
 - D. Microsoft Sentinel
13. A policy must retain project documents for five years and then delete them automatically.
- A. Data Lifecycle Management
 - B. Communication Compliance
 - C. Defender XDR
 - D. Conditional Access
14. An administrator is eligible for the Global Administrator role but must request activation and provide justification before using it.
- A. Privileged Identity Management
 - B. Single sign-on
 - C. Data Loss Prevention
 - D. Microsoft Intune
15. Users must complete MFA when accessing Microsoft 365 from outside trusted locations.
- A. Conditional Access
 - B. Sensitivity labels
 - C. Audit
 - D. Retention
16. Which statement correctly describes Intune and Conditional Access?
- A. Intune determines compliance; Conditional Access can require a compliant device
 - B. Conditional Access determines compliance; Intune grants access
 - C. Both products only protect email
 - D. Intune and Conditional Access are the same feature

17. In Microsoft Entra ID, what does an enterprise application normally represent?
- A. The local service principal instance of an application in a tenant
 - B. A document sensitivity classification
 - C. A device compliance policy
 - D. A SharePoint library
18. In Microsoft Entra ID, what does an app registration primarily define?
- A. The application identity and authentication configuration
 - B. A mailbox retention policy
 - C. A DLP policy alert
 - D. A Teams channel
19. Which capability allows a user to sign in once and access multiple connected applications without repeatedly entering credentials?
- A. Single sign-on
 - B. Data Loss Prevention
 - C. eDiscovery
 - D. Retention
20. A user reports repeated prompts and blocked access after a sign-in. Which information should an administrator review first?
- A. Sign-in logs, Conditional Access results and risky sign-in details
 - B. Retention labels and eDiscovery cases
 - C. DLP policy tips only
 - D. Copilot agent usage
21. A site contains highly confidential content. Access should be limited to members of a specified security group even when individual files were previously shared more broadly.
- A. Restricted access control
 - B. Exchange transport rules
 - C. Identity Secure Score
 - D. Communication Compliance
22. Which report is most suitable for finding SharePoint sites with broad or potentially excessive access?
- A. Data access governance report
 - B. Defender exposure report
 - C. Exchange message trace
 - D. Intune device report
23. Which product correlates alerts from endpoint, identity, email and cloud applications into incidents?
- A. Microsoft Defender XDR
 - B. Microsoft Purview eDiscovery
 - C. Microsoft Intune
 - D. Copilot Analytics
24. A user asks why Copilot referenced a document they did not expect to see. What is the most important first check?
- A. Whether the user already has permission to the document
 - B. Whether the document has a retention label
 - C. Whether the user owns a managed device
 - D. Whether an agent was approved

25. What role does Microsoft Graph play in Microsoft 365 Copilot?

- A. It provides access to authorised Microsoft 365 context and relationships
- B. It replaces all SharePoint permissions
- C. It automatically encrypts every Copilot response
- D. It is a device compliance engine

PRACTICE EXAM 3

25 mixed questions | Select the single best answer for each question

1. An organisation wants predictable per-user access to Microsoft 365 Copilot. Which commercial model is most appropriate?
 - A. A monthly per-user licence
 - B. A retention policy
 - C. A DLP rule
 - D. An enterprise application
2. Where would an administrator typically assign a Microsoft 365 Copilot licence to a user?
 - A. Microsoft 365 admin centre
 - B. Microsoft Purview portal
 - C. Defender portal
 - D. SharePoint site contents
3. An organisation wants selected Copilot experiences billed according to consumption rather than a monthly user licence.
 - A. Configure a pay-as-you-go billing policy
 - B. Create a sensitivity label
 - C. Enable PIM
 - D. Create an eDiscovery case
4. Which source is most useful for reviewing Copilot adoption trends across departments?
 - A. Copilot Analytics and Microsoft 365 usage reports
 - B. Audit only
 - C. Exchange message trace
 - D. Intune app inventory
5. Which task is part of prompt management for supported Microsoft 365 Copilot experiences?
 - A. Save, share, schedule or delete prompts
 - B. Configure switch port VLANs
 - C. Create a Windows Autopilot profile
 - D. Assign a retention period to a mailbox database
6. Which capability is best suited to conducting multi-step research and producing a cited synthesis from work and web sources?
 - A. Researcher
 - B. Analyst
 - C. Communication Compliance
 - D. Defender XDR
7. Which capability is best suited to analysing structured data, identifying trends and generating analytical outputs?
 - A. Analyst
 - B. Researcher
 - C. PIM
 - D. eDiscovery

8. A support team wants an assistant that answers questions only from approved troubleshooting articles.
- A. Create a custom agent grounded in the approved knowledge
 - B. Create a distribution group
 - C. Enable Communication Compliance
 - D. Create an Intune compliance policy
9. After an agent is created, an administrator must decide who can use it. What should be configured?
- A. User access to the agent
 - B. A retention policy
 - C. Identity Secure Score
 - D. A mailbox rule
10. An organisation requires custom agents to be reviewed before general availability. Which process is relevant?
- A. Agent approval
 - B. eDiscovery hold
 - C. Device compliance
 - D. Message trace
11. Which information is most relevant when monitoring an agent after deployment?
- A. Usage, operational insights and lifecycle status
 - B. Only the creator's password age
 - C. Only mailbox quota
 - D. Only device serial numbers
12. Which admin centre is particularly relevant to Power Platform environments and aspects of agent administration?
- A. Power Platform admin centre
 - B. Exchange admin centre
 - C. Teams admin centre
 - D. Windows Settings
13. An administrator needs to review organisation-wide domain names and Microsoft 365 settings.
- A. Microsoft 365 admin centre
 - B. Defender portal
 - C. Microsoft Purview portal
 - D. Power Platform maker portal
14. Which object should be managed in the Exchange admin centre?
- A. Shared mailbox
 - B. SharePoint library
 - C. Conditional Access policy
 - D. Sensitivity label
15. Which object should be managed in the SharePoint admin centre?
- A. SharePoint site
 - B. Enterprise application
 - C. Distribution group
 - D. Defender incident

16. Which object should be managed in the Teams admin centre?
- A. Teams meeting policy
 - B. Retention label
 - C. App registration
 - D. DLP alert investigation
17. Copilot surfaces salary information from a SharePoint file that was accidentally shared with everyone. What should the organisation fix first?
- A. The underlying SharePoint permissions and oversharing
 - B. The user's monitor settings
 - C. The Copilot prompt length
 - D. The Exchange mailbox quota
18. A DLP policy generated an alert after a user attempted to send sensitive information externally. What should an administrator review?
- A. The DLP alert and related activity
 - B. Only Identity Secure Score
 - C. Only the agent approval queue
 - D. Only Exchange mailbox size
19. Which tool provides compliance assessments and recommended improvement actions?
- A. Compliance Manager
 - B. Activity Explorer
 - C. Defender for Endpoint
 - D. Intune Company Portal
20. Which statement best distinguishes Microsoft Purview from Microsoft Defender?
- A. Purview focuses on data governance and compliance; Defender focuses on threats and attacks
 - B. Purview manages device drivers; Defender manages licences
 - C. Purview is only for email; Defender is only for SharePoint
 - D. They are identical products
21. A user proves their identity by entering a password and approving an MFA request. What process occurred?
- A. Authentication
 - B. Authorisation
 - C. Retention
 - D. Classification
22. A user is signed in successfully but cannot open a restricted SharePoint site. What controls this outcome?
- A. Authorisation and permissions
 - B. Authentication only
 - C. DLP detection only
 - D. Copilot Analytics
23. Which authentication method adds a second verification factor beyond a password?
- A. Multifactor authentication
 - B. Single sign-on
 - C. Retention
 - D. Data Explorer

24. Which feature reduces standing administrative privilege by requiring temporary role activation?

- A. Privileged Identity Management
- B. DLP
- C. Communication Compliance
- D. Microsoft Graph

25. Which set lists Microsoft responsible AI principles?

- A. Fairness, reliability and safety, privacy and security, inclusiveness, transparency, accountability
- B. Speed, storage, bandwidth, licensing, uptime, compression
- C. Routing, switching, VLANs, NAT, DNS, DHCP
- D. Retention, eDiscovery, audit, PIM, SSO, MFA

PRACTICE EXAM 4

25 mixed questions | Select the single best answer for each question

1. A confidential document must remain encrypted wherever it is stored. Which feature is the best fit?
 - A. Sensitivity label
 - B. Data Loss Prevention
 - C. Sensitive Information Type
 - D. Audit

2. A policy must stop a confidential document from being shared with external recipients. Which feature is the best fit?
 - A. Data Loss Prevention
 - B. Sensitivity label only
 - C. Audit
 - D. Identity Secure Score

3. A service needs to recognise Australian tax file numbers in documents. Which feature provides the detection logic?
 - A. Sensitive Information Type
 - B. Sensitivity label
 - C. Retention policy
 - D. PIM

4. A document must automatically receive a Confidential label when a sensitive data pattern is detected. Which capability provides the classification and protection outcome?
 - A. Auto-labelling with a sensitivity label
 - B. Audit
 - C. Conditional Access
 - D. Defender XDR

5. An organisation wants to require compliant devices before users access SharePoint. Which service enforces the access requirement?
 - A. Conditional Access
 - B. Microsoft Intune
 - C. Sensitivity labels
 - D. eDiscovery

6. Which service determines whether a device is compliant with password, encryption and operating system requirements?
 - A. Microsoft Intune
 - B. Conditional Access
 - C. Microsoft Purview
 - D. Microsoft Defender XDR

7. An incident joins alerts from a malicious email, suspicious identity activity and malware on a laptop. Which service created the unified incident view?
 - A. Microsoft Defender XDR
 - B. Microsoft Purview eDiscovery
 - C. Microsoft Intune
 - D. Copilot Analytics

8. A legal investigator needs to collect communications relevant to litigation. Which service is most appropriate?
- A. Microsoft Purview eDiscovery
 - B. Microsoft Defender XDR
 - C. Microsoft Intune
 - D. Identity Secure Score
9. Which product is associated most directly with people, identities and access?
- A. Microsoft Entra ID
 - B. Microsoft Intune
 - C. Microsoft Purview
 - D. Microsoft Defender
10. Which product is associated most directly with managed devices and compliance state?
- A. Microsoft Intune
 - B. Microsoft Entra ID
 - C. Microsoft Purview
 - D. Microsoft 365 Copilot
11. Which product is associated most directly with data governance, classification and compliance?
- A. Microsoft Purview
 - B. Microsoft Defender
 - C. Microsoft Intune
 - D. Microsoft Entra ID
12. Which product is associated most directly with detecting and responding to attacks?
- A. Microsoft Defender
 - B. Microsoft Purview
 - C. Microsoft Intune
 - D. Microsoft Exchange
13. Which product provides a general AI assistant across Microsoft 365 applications?
- A. Microsoft 365 Copilot
 - B. A custom agent only
 - C. Microsoft Intune
 - D. Microsoft Purview Audit
14. Which solution is normally created for a specific business process or knowledge source?
- A. A custom agent
 - B. Conditional Access
 - C. A retention label
 - D. Identity Secure Score
15. Which feature should be reviewed to understand recommendations for improving identity security posture?
- A. Identity Secure Score
 - B. Compliance Manager
 - C. Copilot Analytics
 - D. Data Explorer
16. Which Purview tool helps an administrator explore where sensitive information has been identified?
- A. Data Explorer
 - B. Activity Explorer
 - C. Defender incident queue
 - D. Intune device inventory

17. Which Purview tool helps an administrator investigate user actions involving sensitive information?
- A. Activity Explorer
 - B. Data Explorer
 - C. Identity Secure Score
 - D. Power Platform admin centre
18. Which feature answers the question, "Who deleted the file and when?"
- A. Audit
 - B. eDiscovery
 - C. Retention
 - D. Sensitivity labels
19. Which feature answers the question, "Which emails and documents are relevant to this court case?"
- A. eDiscovery
 - B. Audit
 - C. Communication Compliance
 - D. PIM
20. Which feature controls how long content must be kept?
- A. Retention
 - B. Conditional Access
 - C. Defender XDR
 - D. Single sign-on
21. Which feature focuses on policy violations in workplace messages?
- A. Communication Compliance
 - B. Insider Risk Management
 - C. DLP
 - D. PIM
22. Which feature focuses on potentially risky user behaviour that may lead to data theft?
- A. Insider Risk Management
 - B. Communication Compliance
 - C. Single sign-on
 - D. Microsoft Graph
23. Which feature focuses on AI usage and AI-related data security posture?
- A. DSPM for AI
 - B. Defender for Endpoint
 - C. PIM
 - D. Exchange message trace
24. Why can Copilot sometimes surface information a user did not realise they could access?
- A. The underlying content was already accessible to the user
 - B. Copilot ignores all permissions
 - C. Copilot grants itself Global Administrator
 - D. Every SharePoint document is public
25. Which statement best summarises Microsoft Graph in the Copilot architecture?
- A. It connects Copilot to authorised organisational context
 - B. It replaces Microsoft Entra ID
 - C. It is a DLP policy type
 - D. It determines device compliance

PRACTICE EXAM 5

25 mixed questions | Select the single best answer for each question

1. A Sensitive Information Type detects a passport number in a document. What has happened at this stage?
 - A. The data pattern has been identified
 - B. The document has automatically been encrypted in every case
 - C. External sharing has automatically been blocked in every case
 - D. The user has been assigned a privileged role

2. A document remains encrypted after it is downloaded and emailed. Which control most likely applied the protection?
 - A. Sensitivity label
 - B. DLP policy tip
 - C. Audit log
 - D. Identity Secure Score

3. A user receives a warning and is then blocked from sending financial data to a personal email address.
 - A. Data Loss Prevention
 - B. eDiscovery
 - C. PIM
 - D. Copilot Analytics

4. A policy detects credit card numbers and automatically applies a Highly Confidential classification. Which two concepts are working together?
 - A. A Sensitive Information Type and a sensitivity label
 - B. PIM and Conditional Access
 - C. Audit and eDiscovery
 - D. Intune and Defender XDR

5. A Finance user cannot open an encrypted file after moving to another department. Which configuration is the most likely cause?
 - A. The sensitivity label grants access only to the Finance group
 - B. A DLP alert deleted the account
 - C. Identity Secure Score blocked the file
 - D. Researcher changed the permissions

6. Security administrators need an alert when users attempt to send protected financial data externally.
 - A. Configure a DLP policy with alerting
 - B. Create an eDiscovery case
 - C. Enable SSO
 - D. Create a Teams channel

7. Which statement best distinguishes retention from backup?
 - A. Retention governs preservation and deletion according to policy; it is not a general disaster-recovery backup
 - B. Retention creates a full system image
 - C. Retention replaces all permissions
 - D. Retention only applies to devices

8. A legal team wants to run a content search across Exchange and SharePoint for a regulatory investigation.
- A. Microsoft Purview eDiscovery
 - B. Microsoft Defender XDR
 - C. Microsoft Intune
 - D. Identity Secure Score
9. A SharePoint site must be limited to a defined group, even if individual content permissions are broader. Which feature is most relevant?
- A. Restricted access control
 - B. Communication Compliance
 - C. Exchange message trace
 - D. Intune compliance policy
10. Which tool should be used first to identify sites with broad access before a Copilot rollout?
- A. SharePoint data access governance reports
 - B. Defender endpoint inventory
 - C. Exchange message trace
 - D. Copilot prompt library
11. Copilot cites a file that a user can open directly but did not know existed. Which statement is accurate?
- A. Copilot used the user's existing access to help discover the file
 - B. Copilot bypassed access control
 - C. The file was automatically made public
 - D. A DLP policy granted access
12. An employee should no longer be able to use a custom agent. What should the administrator change?
- A. The user access configuration for the agent
 - B. The retention period
 - C. The SIT confidence level
 - D. The device serial number
13. A custom agent is awaiting organisational review before it can be made widely available.
- A. Complete the agent approval process
 - B. Create a DLP alert
 - C. Run an Exchange message trace
 - D. Reset Identity Secure Score
14. An administrator is reviewing whether an unused agent should be retained, updated or retired.
- A. Agent lifecycle management
 - B. Conditional Access
 - C. Data classification
 - D. Single sign-on
15. A user wants a recurring prompt to run on a schedule in a supported Copilot experience.
- A. Use prompt scheduling
 - B. Create a retention label
 - C. Enable PIM
 - D. Configure a device compliance policy
16. Which scenario is most suitable for pay-as-you-go Copilot or agent consumption?
- A. A supported workload where usage should be billed according to consumption
 - B. Encrypting every payroll document
 - C. Investigating a Defender incident
 - D. Requiring MFA for all administrators

17. A manager needs a detailed synthesis of a complex topic using multiple sources and citations.
- A. Researcher
 - B. Analyst
 - C. Communication Compliance
 - D. PIM
18. A finance team needs help analysing a large spreadsheet and finding trends and anomalies.
- A. Analyst
 - B. Researcher
 - C. eDiscovery
 - D. Sensitivity labels
19. A security incident includes an identity alert, a phishing message and an endpoint detection. Which product should correlate them?
- A. Microsoft Defender XDR
 - B. Microsoft Purview Data Explorer
 - C. Microsoft Intune
 - D. Copilot Analytics
20. A sign-in is marked risky and access should be allowed only after MFA. Which policy should enforce this?
- A. Conditional Access
 - B. DLP
 - C. Retention
 - D. Communication Compliance
21. A privileged role should be available only when needed and expire automatically after activation.
- A. Privileged Identity Management
 - B. Single sign-on
 - C. Sensitivity labels
 - D. DSPM for AI
22. Which statement correctly distinguishes app registrations from enterprise applications?
- A. An app registration defines the application identity; an enterprise application is the tenant service principal used for access and assignment
 - B. They are two names for a sensitivity label
 - C. An enterprise application determines device compliance
 - D. An app registration is a SharePoint site
23. Which action best represents the Zero Trust principle "verify explicitly"?
- A. Evaluate identity, device, location and risk signals for each access request
 - B. Trust all devices connected to the office network
 - C. Disable MFA for administrators
 - D. Assume internal traffic is safe
24. Which action best represents the Zero Trust principle "use least-privilege access"?
- A. Grant only the permissions required and use time-limited elevation where possible
 - B. Give every administrator Global Administrator permanently
 - C. Make all SharePoint sites public
 - D. Disable Conditional Access

25. Which action best represents the Zero Trust principle "assume breach"?
- A. Design controls to limit impact and continuously monitor for compromise
 - B. Assume authenticated users cannot be malicious
 - C. Stop collecting security telemetry
 - D. Trust every corporate device indefinitely

COMPLETE ANSWER KEY

How to review

Do not stop at the answer letter. Read the rationale and identify the clue in the scenario that points to the correct feature.

Repeated mistakes are usually caused by product-boundary confusion rather than missing definitions.

PRACTICE EXAM 1 - ANSWERS

1. B - Conditional Access

Conditional Access can evaluate sign-in risk and require MFA before access is granted.

2. A - Audit

Audit records user and administrator activities, including file deletion events.

3. B - Sensitive Information Types

Sensitive Information Types recognise patterns such as credit card numbers and government identifiers.

4. B - Sensitivity labels

Sensitivity labels can encrypt content and restrict access to selected users or groups.

5. A - Data Loss Prevention

DLP policies can detect sensitive content and prevent inappropriate external sharing.

6. B - Data Lifecycle Management

Data Lifecycle Management uses retention policies and labels to retain or delete content according to policy.

7. B - The user already had permission to access the document

Copilot works with the user's existing Microsoft 365 permissions and does not grant new access.

8. A - Microsoft Defender XDR

Defender XDR correlates signals across email, identities, endpoints and other supported services.

9. B - Microsoft Purview eDiscovery

eDiscovery is designed to search, preserve, collect and review content for legal or investigative matters.

10. A - A SharePoint data access governance report

Data access governance reports help identify broad access and possible oversharing in SharePoint.

11. B - Privileged Identity Management

PIM provides eligible, time-limited and just-in-time activation of privileged roles.

12. A - Copilot Analytics and usage reports

Copilot Analytics and Microsoft 365 usage reports provide adoption and usage information.

13. B - A custom agent

A custom agent can be grounded in approved organisational content for a specific business purpose.

14. A - Compliance Manager

Compliance Manager assesses compliance posture and provides improvement recommendations.

15. A - Insider Risk Management

Insider Risk Management identifies and investigates risky user activity.

16. A - Communication Compliance

Communication Compliance evaluates workplace communications for policy violations and inappropriate content.

17. A - DSPM for AI

Microsoft Purview DSPM for AI helps discover AI activity and assess associated data security risks.

18. B - Exchange admin centre

Mailboxes and distribution groups are Exchange objects.

19. B - SharePoint admin centre

The SharePoint admin centre manages sites, sharing, permissions and governance settings.

20. A - Agent user access

Agent access settings determine which users are permitted to use an agent.

21. A - Whether an appropriate Copilot licence is assigned

Access to licensed Copilot capabilities depends on the correct licence being assigned to the user or group.

22. A - Teams admin centre

Teams, channels and Teams policies are managed in the Teams admin centre.

23. B - App registration

An app registration defines the application identity and its authentication and API configuration.

24. A - To measure identity security posture and recommend improvements

Identity Secure Score measures identity-related security posture and recommends actions to improve it.

25. B - Verify explicitly and use least-privilege access

Zero Trust is based on verifying explicitly, using least privilege and assuming breach.

PRACTICE EXAM 2 - ANSWERS

1. A - Microsoft Entra ID

Microsoft Entra ID provides cloud identity and access management.

2. B - Microsoft Intune

Intune evaluates device compliance against configured compliance policies.

3. B - Sensitivity labels

Sensitivity labels classify and protect the item itself, including through persistent encryption.

4. A - Sensitive Information Types

SITs detect recognised patterns and supporting evidence associated with sensitive information.

5. B - Data Loss Prevention

DLP can prevent users from sharing sensitive content with inappropriate recipients.

6. A - Audit

Audit logs record user and administrator activities for investigation.

7. A - eDiscovery

eDiscovery supports preservation, search, collection and review for legal matters.

8. A - Insider Risk Management

Insider Risk Management correlates signals to identify potentially risky internal activities.

9. A - Communication Compliance

Communication Compliance identifies potential policy violations in workplace communications.

10. A - DSPM for AI

DSPM for AI focuses on AI usage, data exposure and AI-related data security posture.

11. A - Activity Explorer

Activity Explorer shows activities associated with sensitive and labelled content.

12. A - Data Explorer

Data Explorer helps identify and explore classified and sensitive content across the environment.

13. A - Data Lifecycle Management

Retention policies and labels in Data Lifecycle Management govern how long content is kept and when it is deleted.

14. A - Privileged Identity Management

PIM supports eligible role assignments with activation requirements such as approval, MFA and justification.

15. A - Conditional Access

Conditional Access evaluates signals such as location and can require MFA.

16. A - Intune determines compliance; Conditional Access can require a compliant device

Intune produces the compliance state, while Conditional Access uses that state in access decisions.

17. A - The local service principal instance of an application in a tenant

An enterprise application is the tenant-specific service principal used to manage access and assignment.

18. A - The application identity and authentication configuration

App registrations define application identities, credentials, redirect URIs and API permissions.

19. A - Single sign-on

SSO lets a user authenticate once and access multiple authorised applications.

20. A - Sign-in logs, Conditional Access results and risky sign-in details

Sign-in logs show authentication results, Conditional Access evaluation and risk information.

21. A - Restricted access control

Restricted access control can limit access to a SharePoint site to specified groups.

22. A - Data access governance report

SharePoint data access governance reports help identify broad access and oversharing risks.

23. A - Microsoft Defender XDR

Defender XDR correlates cross-domain security alerts into a unified incident view.

24. A - Whether the user already has permission to the document

Copilot grounds responses in content available through the user's existing permissions.

25. A - It provides access to authorised Microsoft 365 context and relationships

Microsoft Graph supplies authorised organisational context such as files, messages, meetings and relationships.

PRACTICE EXAM 3 - ANSWERS

1. A - A monthly per-user licence

The monthly licence model provides licensed Copilot capabilities to assigned users.

2. A - Microsoft 365 admin centre

User and group licence assignment is a core Microsoft 365 admin centre task.

3. A - Configure a pay-as-you-go billing policy

Pay-as-you-go supports consumption-based billing for supported Copilot and agent scenarios.

4. A - Copilot Analytics and Microsoft 365 usage reports

Copilot Analytics and usage reports provide adoption and usage insights.

5. A - Save, share, schedule or delete prompts

The current AB-900 outline includes managing prompts by saving, sharing, scheduling and deleting them.

6. A - Researcher

Researcher is intended for complex, multi-step research and synthesis tasks.

7. A - Analyst

Analyst is designed for data analysis, calculation and insight generation.

8. A - Create a custom agent grounded in the approved knowledge

A custom agent can be grounded in selected organisational knowledge for a specific support scenario.

9. A - User access to the agent

Agent user access controls determine who can discover and use the agent.

10. A - Agent approval

Agent approval processes help govern which agents are permitted for organisational use.

11. A - Usage, operational insights and lifecycle status

Agent monitoring includes usage, operational insights and lifecycle management.

12. A - Power Platform admin centre

The Power Platform admin centre manages environments and operational aspects of Power Platform-based agents.

13. A - Microsoft 365 admin centre

The Microsoft 365 admin centre is used for organisation settings, domains, users and licences.

14. A - Shared mailbox

Mailboxes and mail-related groups are Exchange objects.

15. A - SharePoint site

The SharePoint admin centre manages sites and SharePoint governance settings.

16. A - Teams meeting policy

Teams policies, teams and channels are managed through the Teams admin centre.

17. A - The underlying SharePoint permissions and oversharing

Copilot did not create the access; correcting the underlying permissions is the primary remediation.

18. A - The DLP alert and related activity

DLP alerts provide the details needed to investigate and respond to possible data loss events.

19. A - Compliance Manager

Compliance Manager helps evaluate compliance posture and prioritise improvement actions.

20. A - Purview focuses on data governance and compliance; Defender focuses on threats and attacks

Purview protects and governs data, while Defender detects and responds to security threats.

21. A - Authentication

Authentication verifies who the user is.

22. A - Authorisation and permissions

Authorisation determines what an authenticated user is allowed to access.

23. A - Multifactor authentication

MFA requires two or more categories of authentication evidence.

24. A - Privileged Identity Management

PIM enables just-in-time privileged role activation instead of permanent access.

25. A - Fairness, reliability and safety, privacy and security, inclusiveness, transparency, accountability

Microsoft responsible AI principles include fairness, reliability and safety, privacy and security, inclusiveness, transparency and accountability.

PRACTICE EXAM 4 - ANSWERS

1. A - Sensitivity label

Sensitivity labels can apply persistent protection to the document itself.

2. A - Data Loss Prevention

DLP is designed to prevent inappropriate use or sharing of sensitive content.

3. A - Sensitive Information Type

SITs provide the pattern and evidence logic used to detect sensitive data types.

4. A - Auto-labelling with a sensitivity label

SITs can be used as conditions, while the sensitivity label provides the resulting classification and protection.

5. A - Conditional Access

Conditional Access uses the device compliance signal to grant or block access.

6. A - Microsoft Intune

Intune evaluates the device against configured compliance policies.

7. A - Microsoft Defender XDR

Defender XDR correlates security signals across multiple protection domains.

8. A - Microsoft Purview eDiscovery

eDiscovery supports legal search, preservation, collection and review.

9. A - Microsoft Entra ID

Entra ID manages identities, authentication and access controls.

10. A - Microsoft Intune

Intune manages endpoints and evaluates device compliance.

11. A - Microsoft Purview

Purview provides data governance, information protection and compliance capabilities.

12. A - Microsoft Defender

Microsoft Defender products focus on threat protection, detection and response.

13. A - Microsoft 365 Copilot

Microsoft 365 Copilot provides broadly integrated AI assistance across Microsoft 365.

14. A - A custom agent

Agents are purpose-built assistants grounded in selected data and instructions.

15. A - Identity Secure Score

Identity Secure Score focuses on identity security controls and recommendations.

16. A - Data Explorer

Data Explorer provides visibility into classified and sensitive content.

17. A - Activity Explorer

Activity Explorer shows activities such as label changes, sharing and DLP-related events.

18. A - Audit

Audit logs record activities performed by users and administrators.

19. A - eDiscovery

eDiscovery searches and collects content relevant to legal and investigative matters.

20. A - Retention

Retention policies and labels govern preservation and deletion periods.

21. A - Communication Compliance

Communication Compliance examines communications for inappropriate or prohibited content.

22. A - Insider Risk Management

Insider Risk Management focuses on user-related risk indicators and activities.

23. A - DSPM for AI

DSPM for AI discovers AI activity and helps manage associated data risks.

24. A - The underlying content was already accessible to the user

Copilot respects existing permissions, but can make already accessible information easier to discover.

25. A - It connects Copilot to authorised organisational context

Graph supplies Microsoft 365 data and relationships within the user's authorised context.

PRACTICE EXAM 5 - ANSWERS

1. A - The data pattern has been identified

A SIT provides detection. Protection or enforcement requires a label, DLP policy or other configured control.

2. A - Sensitivity label

Sensitivity label encryption can travel with the content beyond its original location.

3. A - Data Loss Prevention

DLP can display policy tips, warn users and block prohibited sharing actions.

4. A - A Sensitive Information Type and a sensitivity label

The SIT supplies detection logic, while the sensitivity label supplies classification and protection.

5. A - The sensitivity label grants access only to the Finance group

Label-based encryption can restrict access to selected users or groups, independent of file location.

6. A - Configure a DLP policy with alerting

DLP can generate alerts when policy conditions and user actions indicate possible data loss.

7. A - Retention governs preservation and deletion according to policy; it is not a general disaster-recovery backup

Retention is a governance control for keeping or deleting content, not a substitute for backup and recovery.

8. A - Microsoft Purview eDiscovery

Content search in eDiscovery can locate relevant emails and files across supported Microsoft 365 locations.

9. A - Restricted access control

Restricted access control limits site access to specified groups and helps contain oversharing.

10. A - SharePoint data access governance reports

Data access governance reports provide visibility into potential SharePoint oversharing.

11. A - Copilot used the user's existing access to help discover the file

Copilot can improve discoverability of content the user is already authorised to access.

12. A - The user access configuration for the agent

Agent access controls determine which users are allowed to use the agent.

13. A - Complete the agent approval process

The approval process is used to review and govern agents before wider use.

14. A - Agent lifecycle management

Lifecycle management includes monitoring, maintaining and retiring agents.

15. A - Use prompt scheduling

Prompt management can include saving, sharing, scheduling and deleting prompts.

16. A - A supported workload where usage should be billed according to consumption

Pay-as-you-go is a consumption-based commercial model for supported Copilot and agent scenarios.

17. A - Researcher

Researcher is intended for multi-step research, synthesis and cited reporting.

18. A - Analyst

Analyst is designed for data analysis and analytical reasoning.

19. A - Microsoft Defender XDR

Defender XDR correlates related alerts across security domains into incidents.

20. A - Conditional Access

Conditional Access can use sign-in risk as a condition and require MFA as a grant control.

21. A - Privileged Identity Management

PIM provides eligible assignments and time-limited activation for privileged roles.

22. A - An app registration defines the application identity; an enterprise application is the tenant service principal used for access and assignment

The app registration defines the application object, while the enterprise application represents its service principal in a tenant.

23. A - Evaluate identity, device, location and risk signals for each access request

Verify explicitly means using all available signals to make an informed access decision.

24. A - Grant only the permissions required and use time-limited elevation where possible

Least privilege limits access to the minimum necessary scope and duration.

25. A - Design controls to limit impact and continuously monitor for compromise

Assume breach means operating as though compromise can occur and limiting its potential impact.

SCORE TRACKER

Use this table to track your first attempt and your score after reviewing weak areas. A high practice score is useful, but it does not guarantee an exam result.

EXAM	FIRST SCORE	REVIEW DATE	SECOND SCORE	TOPIC TO REVISE
1				
2				
3				
4				
5				

OFFICIAL REFERENCES

The question bank was aligned to the public AB-900 objectives available in July 2026. Microsoft Learn remains the authoritative source for current exam objectives and product documentation.

- [AB-900 certification page](#)
- [AB-900 study guide](#)
- [Microsoft certification practice assessments](#)
- [Microsoft Certification Exam Candidate Agreement](#)

Microsoft, Microsoft 365, Copilot, Entra, Intune, Purview and Defender are trademarks of the Microsoft group of companies. This independent resource is not affiliated with or endorsed by Microsoft.