Study guide for Exam MS-500: Microsoft 365 Security Administration

Purpose of this document

This study guide should help you understand what to expect on the exam and includes a summary of the topics the exam might cover and links to additional resources. The information and materials in this document should help you focus your studies as you prepare for the exam.

Useful links	Description
Review the skills measured as of November 4, 2022	This list represents the skills measured AFTER the date provided. Study this list if you plan to take the exam AFTER that date.
Review the skills measured prior to November 4, 2022	Study this list of skills if you take your exam PRIOR to the date provided.
Change log	You can go directly to the change log if you want to see the changes that will be made on the date provided.
How to earn the certification	Some certifications only require passing one exam, while others require passing multiple exams.
Certification renewal	Microsoft associate, expert, and specialty certifications expire annually. You can renew by passing a **free** online assessment on Microsoft Learn.
Your Microsoft Learn profile	Connecting your certification profile to Learn allows you to schedule and renew exams and share and print certificates.
Passing score	A score of 700 or greater is required to pass.
Exam sandbox	You can explore the exam environment by visiting our exam sandbox.
Request accommodations	If you use assistive devices, require extra time, or need modification to any part of the exam experience, you can request an accommodation.

Useful links	Description
Take a practice test	Are you ready to take the exam or do you need to study a bit more?

Updates to the exam

Our exams are updated periodically to reflect skills that are required to perform a role. We have included two versions of the Skills Measured objectives depending on when you are taking the exam.

We always update the English language version of the exam first. Some exams are localized into other languages, and those are updated approximately eight weeks after the English version is updated. Other available languages are listed in the **Schedule Exam** section of the **Exam Details** webpage. If the exam isn't available in your preferred language, you can request an additional 30 minutes to complete the exam.

Note

The bullets that follow each of the skills measured are intended to illustrate how we are assessing that skill. Related topics may be covered in the exam.

Note

Most questions cover features that are general availability (GA). The exam may contain questions on Preview features if those features are commonly used.

Skills measured as of November 4, 2022

Audience Profile

Candidates for this exam plan, implement, manage, and monitor security and compliance solutions for Microsoft 365 and hybrid environments. The Microsoft 365 security administrator proactively secures identity and access, implements threat protection, manages information protection, and enforces compliance. The Microsoft 365 security administrator collaborates with the Microsoft 365 enterprise administrator, business stakeholders, and other workload administrators to plan and implement security strategies.

Candidates for this exam have functional experience with Microsoft 365 workloads and with Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra. They have implemented security for Microsoft 365 environments, including hybrid environments. They have a working knowledge of Windows clients, Windows servers, Active Directory, and PowerShell.

- Implement and manage identity and access (25–30%)
- Implement and manage threat protection (30–35%)
- Implement and manage information protection (15–20%)
- Manage compliance in Microsoft 365 (20–25%)

Implement and manage identity and access (25–30%)

Plan and implement identity and access for Microsoft 365 hybrid environments

- Choose an authentication method to connect to a hybrid environment
- Plan and implement pass-through authentication and password hash sync
- Plan and implement Azure AD synchronization for hybrid environments
- Monitor and troubleshoot Azure AD Connect events

Plan and implement identities in Azure AD

- Implement Azure AD group membership
- Implement password management, including self-service password reset and Azure AD Password Protection
- Manage external identities in Azure AD and Microsoft 365 workloads
- Plan and implement roles and role groups
- Audit Azure AD

Implement authentication methods

- Implement multi-factor authentication (MFA) by using conditional access policies
- Manage and monitor MFA
- Plan and implement Windows Hello for Business, FIDO, and passwordless authentication

Plan and implement conditional access

- Plan and implement conditional access policies
- Plan and implement device compliance policies
- Test and troubleshoot conditional access policies

Configure and manage identity governance

- Implement Azure AD Privileged Identity Management
- Implement and manage entitlement management
- Implement and manage access reviews

Implement Azure AD Identity Protection

- Implement user risk policy
- Implement sign-in risk policy
- Configure Identity Protection alerts
- Review and respond to risk events

Implement and manage threat protection (30–35%)

Secure identity by using Microsoft Defender for Identity

- Plan a Microsoft Defender for Identity solution
- Install and configure Microsoft Defender for Identity

- Manage and monitor Microsoft Defender for Identity
- Secure score
- Analyze identity-related threats and risks identified in Microsoft 365 Defender

Secure endpoints by using Microsoft Defender for Endpoint

- Plan a Microsoft Defender for Endpoint solution
- Implement Microsoft Defender for Endpoint
- Manage and monitor Microsoft Defender for Endpoint
- Analyze and remediate threats and risks to endpoints identified in Microsoft 365 Defender

Secure endpoints by using Microsoft Endpoint Manager

- Plan for device and application protection
- Configure and manage Microsoft Defender Application Guard
- Configure and manage Windows Defender Application Control
- Configure and manage exploit protection
- Configure and manage device encryption
- Configure and manage application protection policies
- Monitor and manage device security status using Microsoft Endpoint Manager admin center
- Analyze and remediate threats and risks to endpoints identified in Microsoft Endpoint Manager

Secure collaboration by using Microsoft Defender for Office 365

- Plan a Microsoft Defender for Office 365 solution
- Configure Microsoft Defender for Office 365
- Monitor for threats by using Microsoft Defender for Office 365
- Analyze and remediate threats and risks to collaboration workloads identified in Microsoft 365 Defender
- Conduct simulated attacks by using Attack simulation training

Detect and respond to threats in Microsoft 365 by using Microsoft Sentinel

- Plan a Microsoft Sentinel solution for Microsoft 365
- Implement and configure Microsoft Sentinel for Microsoft 365
- Manage and monitor Microsoft 365 security by using Microsoft Sentinel
- Respond to threats using built-in playbooks in Microsoft Sentinel

Secure connections to cloud apps by using Microsoft Defender for Cloud Apps

- Plan Microsoft Defender for Cloud Apps implementation
- Configure Microsoft Defender for Cloud Apps
- Manage cloud app discovery
- Manage entries in the Microsoft Defender for Cloud Apps catalog
- Manage apps in Microsoft Defender for Cloud Apps
- Configure Microsoft Defender for Cloud Apps connectors and OAuth apps

- Configure Microsoft Defender for Cloud Apps policies and templates
- Analyze and remediate threats and risks relating to cloud app connections identified in Microsoft 365 Defender
- Manage App governance in Microsoft Defender for Cloud Apps

Implement and manage information protection (15–20%)

Manage sensitive information

- Plan a sensitivity label solution
- Create and manage sensitive information types
- Configure sensitivity labels and policies
- Publish sensitivity labels to Microsoft 365 workloads
- Monitor data classification and label usage by using Content explorer and Activity explorer
- Apply labels to files and schematized data assets in Microsoft Purview Data Map

Implement and manage Microsoft Purview Data Loss Prevention (DLP)

- Plan a DLP solution
- Create and manage DLP policies for Microsoft 365 workloads
- Implement and manage Endpoint DLP
- Monitor DLP
- Respond to DLP alerts and notifications

Plan and implement Microsoft Purview Data lifecycle management

- Plan for data lifecycle management
- Review and interpret data lifecycle management reports and dashboards
- Configure retention labels, policies, and label policies
- Plan and implement adaptive scopes
- Configure retention in Microsoft 365 workloads
- Find and recover deleted Office 365 data

Manage compliance in Microsoft 365 (20–25%)

Manage and analyze audit logs and reports in Microsoft Purview

- Plan for auditing and reporting
- Investigate compliance activities by using audit logs
- Review and interpret compliance reports and dashboards
- Configure alert policies
- Configure audit retention policies

Plan for, conduct, and manage eDiscovery cases

- Recommend eDiscovery Standard or Premium
- Plan for content search and eDiscovery

- Delegate permissions to use search and discovery tools
- Use search and investigation tools to discover and respond
- Manage eDiscovery cases

Manage regulatory and privacy requirements

- Plan for regulatory compliance in Microsoft 365
- Manage regulatory compliance in the Microsoft Purview Compliance Manager
- Implement privacy risk management in Microsoft Priva
- Implement and manage Subject Rights Requests in Microsoft Priva

Manage insider risk solutions in Microsoft 365

- Implement and manage Customer Lockbox
- Implement and manage Communication compliance policies
- Implement and manage Insider risk management policies
- Implement and manage Information barrier policies
- Implement and manage Privileged access management

Study Resources

We recommend that you train and get hands-on experience before you take the exam. We offer self-study options and classroom training as well as links to documentation, community sites, and videos.

Study resources	Links to learning and documentation
Get trained	Choose from self-paced learning paths and modules or take an instructor-led course
Find documentation	Microsoft 365 documentation Azure Active Directory documentation Microsoft 365 Defender documentation Microsoft Defender for Identity documentation Microsoft Defender for Endpoint documentation Microsoft Sentinel documentation Learn about data loss prevention
Ask a question	Microsoft Q&A | Microsoft Docs
Get community support	Microsoft 365 - Microsoft Tech Community
Follow Microsoft Learn	Microsoft Learn - Microsoft Tech Community

Study resources	Links to learning and documentation
Find a video	Exam Readiness Zone

Change log

Key to understanding the table: The topic groups (also known as functional groups) are in bold typeface followed by the objectives within each group. The table is a comparison between the two versions of the exam skills measured and the third column describes the extent of the changes.

Skill area prior to November 4, 2022	Skill area as of November 4, 2022	Changes
Audience Profile		Major
Implement and manage identity and access	**Implement and manage identity and access**	% of exam decreased
Secure Microsoft 365 hybrid environments	Plan and implement identity and access for Microsoft 365 hybrid environments	Major
Secure identities	Plan and implement identities in Azure AD	Major
Implement authentication methods	Implement authentication methods	Minor
Implement conditional access	Plan and implement conditional access	Minor
Implement roles and role groups	-	Removed
Configure and manage identity governance	Configure and manage identity governance	Minor
-	Implement Azure AD Identity Protection	Added
Implement and manage threat protection	**Implement and manage threat protection**	% of exam increased
Implement Azure AD Identity Protection	-	Removed
Implement and manage Microsoft Defender for Identity	Secure identity by using Microsoft Defender for Identity	Minor
Implement and manage Microsoft Defender for Endpoint	Secure endpoints by using Microsoft Defender for Endpoint	Minor

Skill area prior to November 4, 2022	Skill area as of November 4, 2022	Changes
Implement and manage by using Microsoft Endpoint Manager	Secure endpoints by using Microsoft Endpoint Manager	Major
Implement and manage Microsoft Defender for Office 365	Secure collaboration by using Microsoft Defender for Office 365	Major
Monitor M365 security with Microsoft Sentinel	Detect and respond to threats in Microsoft 365 by using Microsoft Sentinel	Major
Implement and manage Microsoft Defender for Cloud Apps	Secure connections to cloud apps by using Microsoft Defender for Cloud Apps	Minor
Implement and manage information protection	**Implement and manage information protection**	% of exam increased
Manage sensitive information	Manage sensitive information	Major
Manage Data Loss Prevention (DLP)	Implement and manage Microsoft Purview Data Loss Prevention (DLP)	Minor
Manage data governance and retention	-	Removed
Plan and implement Microsoft Purview Data lifecycle management	Plan and implement Microsoft Purview Data lifecycle management	New
Manage governance and compliance features in Microsoft 365	**Manage compliance in Microsoft 365**	No change
Configure and analyze security reporting	-	Removed
Manage and analyze audit logs and reports	Manage and analyze audit logs and reports in Microsoft Purview	Minor
Discover and respond to compliance queries in Microsoft 365		Removed
-	Plan for, conduct, and manage eDiscovery cases	New
Manage regulatory compliance	Manage regulatory and privacy requirements	Major
Manage insider risk solutions in Microsoft 365	Manage insider risk solutions in Microsoft 365	Minor

Skills measured prior to November 4, 2022

- Implement and manage identity and access (35–40%)
- Implement and manage threat protection (25–30%)
- Implement and manage information protection (10–15%)
- Manage governance and compliance features in Microsoft 365 (20–25%)

Implement and manage identity and access (35–40%)

Secure Microsoft 365 hybrid environments

- Plan Azure AD authentication options
- Plan Azure AD synchronization options
- Monitor and troubleshoot Azure AD Connect events

Secure Identities

- Implement Azure AD group membership
- Implement password management
- Manage external identities in Azure AD and Microsoft 365 workloads

Implement authentication methods

- Implement multi-factor authentication (MFA) by using conditional access policy
- Manage and monitor MFA
- Plan and implement device authentication methods like Windows Hello

Implement conditional access

- Plan for compliance and conditional access policies
- Configure and manage device compliance policies
- Implement and manage conditional access
- Test and troubleshoot conditional access policies

Implement roles and role groups

- Plan for roles and role groups
- Configure roles and role groups
- Audit roles for least privileged access

Configure and manage identity governance

- Implement Azure AD Privileged Identity Management
- Implement and manage entitlement management
- Implement and manage access reviews

Implement Azure AD Identity Protection

- Implement user risk policy
- Implement sign-in risk policy

- Configure Identity Protection alerts
- Review and respond to risk events

Implement and manage threat protection (25–30%)

Implement and manage Microsoft Defender for Identity

- Plan a Microsoft Defender for Identity solution
- Install and configure Microsoft Defender for Identity
- Monitor and manage Microsoft Defender for Identity

Implement device threat protection

- Plan a Microsoft Defender for Endpoint solution
- Implement Microsoft Defender for Endpoint
- Manage and monitor Microsoft Defender for Endpoint

Implement and manage device and application protection

- Plan for device and application protection
- Configure and manage Microsoft Defender Application Guard
- Configure and manage Microsoft Defender Application Control
- Configure and manage exploit protection
- Configure and manage Windows device encryption
- Configure and manage non-Windows device encryption
- Implement application protection policies
- Configure and manage device compliance for endpoint security

Implement and manage Microsoft Defender for Office 365

- Configure Microsoft Defender for Office 365
- Monitor for and remediate threats using Microsoft Defender for Office 365
- Conduct simulated attacks using Attack simulation training

Monitor Microsoft 365 Security with Microsoft Sentinel

- Plan and implement Microsoft Sentinel
- Configure playbooks in Microsoft Sentinel
- Manage and monitor with Microsoft Sentinel
- Respond to threats using built-in playbooks in Microsoft Sentinel

Implement and manage Microsoft Defender for Cloud Apps

- Plan Microsoft Defender for Cloud Apps implementation
- Configure Microsoft Defender for Cloud Apps
- Manage cloud app discovery
- Manage entries in the Microsoft Defender for Cloud Apps catalog
- Manage apps in Microsoft Defender for Cloud Apps

- Configure Microsoft Defender Cloud Apps connectors and OAuth apps
- Configure Microsoft Defender for Cloud Apps policies and templates
- Review, interpret and respond to Microsoft Defender for Cloud Apps alerts, reports, dashboards, and logs

Implement and manage information protection (10–15%)

Manage sensitive information

- Plan a sensitivity label solution
- Create and manage sensitive information types
- Configure sensitivity labels and policies
- Configure and use Activity Explorer
- Use sensitivity labels with Teams, SharePoint, OneDrive, and Office apps

Manage Data Loss Prevention (DLP)

- Plan a DLP solution
- Create and manage DLP policies for Microsoft 365 workloads
- Create and manage sensitive information types
- Monitor DLP reports
- Manage DLP notifications
- Implement Endpoint DLP

Manage data governance and retention

- Plan for data governance and retention
- Review and interpret data governance reports and dashboards
- Configure retention labels and policies
- Configure retention in Microsoft 365 workloads
- Find and recover deleted Office 365 data
- Configure and use Microsoft 365 Records Management

Manage governance and compliance features in Microsoft 365 (20–25%)

Configure and analyze security reporting

- Monitor and manage device security status using Microsoft Endpoint Manager admin center
- Manage and monitor security reports and dashboards using Microsoft 365 Defender portal
- Plan for custom security reporting with Graph Security API
- Use secure score dashboards to review actions and recommendations

Manage and analyze audit logs and reports

- Plan for auditing and reporting
- Perform audit log search

- Review and interpret compliance reports and dashboards
- Configure alert policies

Discover and respond to compliance queries in Microsoft 365

- Plan for content search and eDiscovery
- Delegate permissions to use search and discovery tools
- Use search and investigation tools to discover and respond
- Manage eDiscovery cases

Manage regulatory compliance

- Plan for regulatory compliance in Microsoft 365
- Manage Data Subject Requests (DSRs)
- Administer Compliance Manager in Microsoft 365 compliance center
- Use Compliance Manager

Manage insider risk solutions in Microsoft 365

- Implement and manage Customer Lockbox
- Implement and manage communication compliance policies
- Implement and manage Insider risk management policies
- Implement and manage information barrier policies
- Implement and manage privileged access management