Exam MS-500: Microsoft 365 Security Administration – Skills Measured

This exam was updated on March 23, 2021. Following the current exam guide, we have included a version of the exam guide with Track Changes set to "On," showing the changes that were made to the exam on that date.

Audience Profile

Candidates for this exam implement, manage, and monitor security and compliance solutions for Microsoft 365 and hybrid environments. The Microsoft 365 Security Administrator proactively secures M365 enterprise environments, responds to threats, performs investigations, and enforces data governance. The Microsoft 365 Security Administrator collaborates with the Microsoft 365 Enterprise Administrator, business stakeholders, and other workload administrators to plan and implement security strategies and ensures that the solutions comply with the policies and regulations of the organization.

Candidates for this exam are familiar with M365 workloads and have strong skills and experience with identity protection, information protection, threat protection, security management, and data governance. This role focuses on the M365 environment and includes hybrid environments.

Skills Measured

NOTE: The bullets that appear below each of the skills measured are intended to illustrate how we are assessing that skill. This list is not definitive or exhaustive.

NOTE: Most questions cover features that are General Availability (GA). The exam may contain questions on Preview features if those features are commonly used.

Implement and manage identity and access (30-35%)

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
- configure and manage identity governance

Implement authentication methods

- plan sign-on security
- implement multi-factor authentication (MFA)
- manage and monitor MFA
- plan and implement device authentication methods like Windows Hello
- configure and manage Azure AD user authentication options and self-service password management

Implement conditional access

- plan for compliance and conditional access policies
- configure and manage device compliance for endpoint security
- implement and manage conditional access

Implement role-based access control (RBAC)

- plan for roles
- configure roles
- audit roles

Implement Azure AD Privileged Identity Management (PIM)

- plan for Azure PIM
- assign eligibility and activate admin roles
- manage Azure PIM role requests and assignments
- monitor PIM history and alerts

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 (20-25%)

Implement an enterprise hybrid threat protection solution

- 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 Secure Boot
- configure and manage Windows device encryption
- configure and manage non-Windows device encryption
- plan for securing applications data on devices
- implement application protection policies

Implement and manage Microsoft Defender for Office 365

- configure Microsoft Defender for Office 365
- monitor Microsoft Defender for Office 365
- conduct simulated attacks using Attack Simulator

Monitor Microsoft 365 Security with Azure Sentinel

- plan and implement Azure Sentinel
- configure playbooks in Azure Sentinel
- manage and monitor Azure Sentinel
- respond to threats in Azure Sentinel

Implement and manage information protection (15-20%)

Secure data access within Office 365

- implement and manage Customer Lockbox
- configure data access in Office 365 collaboration workloads
- configure B2B sharing for external users

Manage sensitivity labels

- plan a sensitivity label solution
- configure sensitivity labels and policies.
- configure and use label analytics
- use sensitivity labels with Teams, Sharepoint, OneDrive and Office apps

Manage Data Loss Prevention (DLP)

- plan a DLP solution
- create and manage DLP policies
- create and manage sensitive information types
- monitor DLP reports
- manage DLP notifications

Implement and manage Microsoft Cloud App Security

- plan Cloud App Security implementation
- configure Microsoft Cloud App Security
- manage cloud app discovery
- manage entries in the Cloud app catalog
- manage apps in Cloud App Security
- manage Microsoft Cloud App Security
- configure Cloud App Security connectors and Oauth apps
- configure Cloud App Security policies and templates
- review, interpret and respond to Cloud App Security alerts, reports, dashboards and logs.

Manage governance and compliance features in Microsoft 365 (25-30%)

Configure and analyze security reporting

- monitor and manage device security status using Microsoft Endpoint Manager Admin Center.
- manage and monitor security and dashboards using Microsoft 365 Security Center
- plan for custom security reporting with Graph Security API
- use secure score dashboards to review actions and recommendations
- configure alert policies

Manage and analyze audit logs and reports

- plan for auditing and reporting
- perform audit log search
- review and interpret compliance reports and dashboards
- configure audit alert policy

Manage data governance and retention

- plan for data governance and retention
- review and interpret data governance reports and dashboards

- configure retention labels and policies
- define data governance event types
- define and manage communication compliance policies
- configure Information holds
- find and recover deleted Office 365 data
- configure data archiving
- manage inactive mailboxes

Manage search and investigation

- plan for content search and eDiscovery
- delegate permissions to use search and discovery tools
- use search and investigation tools to perform content searches
- export content search results
- manage eDiscovery cases

Manage data privacy regulation compliance

- plan for regulatory compliance in Microsoft 365
- review and interpret GDPR dashboards and reports
- manage Data Subject Requests (DSRs)
- administer Compliance Manager in Microsoft 365 compliance center
- review Compliance Manager reports
- create and perform Compliance Manager assessments and action items

The exam guide below shows the changes that were implemented on March 23, 2021.

Audience Profile

Candidates for this exam implement, manage, and monitor security and compliance solutions for Microsoft 365 and hybrid environments. The Microsoft 365 Security Administrator proactively secures M365 enterprise environments, responds to threats, performs investigations, and enforces data governance. The Microsoft 365 Security Administrator collaborates with the Microsoft 365 Enterprise Administrator, business stakeholders, and other workload administrators to plan and implement security strategies and ensures that the solutions comply with the policies and regulations of the organization.

Candidates for this exam are familiar with M365 workloads and have strong skills and experience with identity protection, information protection, threat protection, security management, and data governance. This role focuses on the M365 environment and includes hybrid environments.

Skills Measured

NOTE: The bullets that appear below each of the skills measured are intended to illustrate how we are assessing that skill. This list is not definitive or exhaustive.

NOTE: Most questions cover features that are General Availability (GA). The exam may contain questions on Preview features if those features are commonly used.

Implement and manage identity and access (30-35%)

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
- configure and manage identity governance

Implement authentication methods

- plan sign-on security
- implement multi-factor authentication (MFA)
- manage and monitor MFA
- plan and implement device authentication methods like Windows Hello
- configure and manage Azure AD user authentication options and self-service password management

Implement conditional access

- plan for compliance and conditional access policies
- configure and manage device compliance for endpoint security
- implement and manage conditional access

Implement role-based access control (RBAC)

- plan for roles
- configure roles
- audit roles

Implement Azure AD Privileged Identity Management (PIM)

- plan for Azure PIM

- assign eligibility and activate admin roles
- manage Azure PIM role requests and assignments
- monitor PIM history and alerts

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 (20-25%)

Implement an enterprise hybrid threat protection solution

- 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 Secure Boot
- configure and manage Windows device encryption
- configure and manage non-Windows device encryption
- plan for securing applications data on devices
- implement application protection policies

Implement and manage Microsoft Defender for Office 365

- configure Microsoft Defender for Office 365
- monitor Microsoft Defender for Office 365
- conduct simulated attacks using Attack Simulator

Monitor Microsoft 365 Security with Azure Sentinel

- plan and implement Azure Sentinel
- configure playbooks in Azure Sentinel
- manage and monitor Azure Sentinel
- respond to threats in Azure Sentinel

Implement and manage information protection (15-20%)

Secure data access within Office 365

- implement and manage Customer Lockbox
- configure data access in Office 365 collaboration workloads
- configure B2B sharing for external users

Manage sensitivity labels

- plan a sensitivity label solution
- configure sensitivity labels and policies.
- configure and use label analytics
- use sensitivity labels with Teams, Sharepoint, OneDrive and Office apps

Manage Data Loss Prevention (DLP)

- plan a DLP solution
- create and manage DLP policies
- create and manage sensitive information types
- monitor DLP reports
- manage DLP notifications

Implement and manage Microsoft Cloud App Security

- plan Cloud App Security implementation
- configure Microsoft Cloud App Security
- manage cloud app discovery
- manage entries in the Cloud app catalog
- manage apps in Cloud App Security
- manage Microsoft Cloud App Security
- configure Cloud App Security connectors and Oauth apps
- configure Cloud App Security policies and templates
- review, interpret and respond to Cloud App Security alerts, reports, dashboards and logs.

Manage governance and compliance features in Microsoft 365 (25-30%)

Configure and analyze security reporting

- monitor and manage device security status using Microsoft Endpoint Manager Admin Center
- manage and monitor security and dashboards using Microsoft 365 Security Center
- plan for custom security reporting with Graph Security API
- use secure score dashboards to review actions and ~~recommendations in the Microsoft 365 security center~~
- configure alert policies

Manage and analyze audit logs and reports

- plan for auditing and reporting
- perform audit log search
- review and interpret compliance reports and dashboards
- configure audit alert policy

Manage data governance and retention

- plan for data governance and retention
- review and interpret data governance reports and dashboards
- configure retention labels and policies
- define data governance event types
- define and manage communication compliance policies
- configure Information holds
- find and recover deleted Office 365 data
- configure data archiving
- manage inactive mailboxes

Manage search and investigation

- plan for content search and eDiscovery
- delegate permissions to use search and discovery tools
- use search and investigation tools to perform content searches
- export content search results
- manage eDiscovery cases

Manage data privacy regulation compliance

- plan for regulatory compliance in Microsoft 365
- review and interpret GDPR dashboards and reports
- manage Data Subject Requests (DSRs)
- administer Compliance Manager in Microsoft 365 compliance ~~security~~ center

- review Compliance Manager reports
- create and perform Compliance Manager assessments and action items