Exam MS-500: Microsoft 365 Security Administration

Skills Measured

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

Secure Microsoft 365 hybrid environments

• configure and manage security integration components in Microsoft 365 hybrid environments, including connectivity, synchronization services, and authentication

• plan Azure AD authentication options

• plan Azure AD synchronization options

• monitor and interpret Azure AD Connect events

Secure user accounts

• implement Azure AD dynamic group membership

• implement Azure AD Self-service password reset

• manage Azure AD access reviews

Implement authentication methods

• plan sign-on security

• implement multi-factor authentication (MFA)

• manage and monitor MFA

• implement device sign-on methods

• manage authentication methods

• monitor authentication methods

Implement conditional access

• plan for compliance and conditional access policies

• configure and manage device compliance policy

• configure and manage conditional access policy

• monitor Conditional Access and Device Compliance

Implement role-based access control (RBAC)

• plan for RBAC

• configure RBAC

• monitor RBAC usage

Implement Azure AD Privileged Identity Management (PIM)

• plan for Azure PIM

• configure and manage Azure PIM

• monitor Azure PIM

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 an Azure Advanced Threat Protection (ATP) solution

• install and configure Azure ATP

• manage Azure ATP workspace health

• generate Azure ATP reports

• integrate Azure ATP with Microsoft Defender ATP

• monitor Azure ATP

• manage suspicious activities

Implement device threat protection

• plan and implement a Microsoft Defender ATP solution

• manage Microsoft Defender ATP

• monitor Microsoft Defender ATP

Implement and manage device and application protection

• plan for device protection

• configure and manage Windows Defender Application Guard

• configure and manage Windows Defender Application Control

• configure and manage Windows Defender Exploit Guard

• configure Secure Boot

• configure and manage Windows 10 device encryption

• configure and manage non-Windows device encryption

• plan for securing applications data on devices

• define managed apps for Mobile Application Management (MAM)

• protect your enterprise data using Windows Information Protection (WIP)

• configure Intune App Protection policies for Windows and non-Windows devices

Implement and manage Office 365 ATP

• configure Office 365 ATP anti-phishing protection

• configure Office 365 ATP anti-phishing policies

• define users and domains to protect with Office 365 ATP Anti-phishing

• configure Office 365 ATP anti-spoofing

• configure actions against impersonation

• configure Office 365 ATP anti-spam protection

• enable Office 365 ATP Safe-Attachments

• configure Office 365 ATP Safe Attachments policies

• configure Office 365 ATP Safe Attachments options

• configure Office 365 ATP Safe Links options

• configure Office 365 ATP Safe Links blocked URLs

• configure Office 365 ATP Safe Links policies

• review threats and malware trends on the Office 365 ATP Threat Management dashboard

• review threats and malware trends with Office 365 ATP Threat Explorer and Threat Tracker

• create and review Office 365 ATP incidents

• review quarantined items in ATP including Microsoft SharePoint Online, OneDrive for Business, Exchange Online, and Microsoft Teams

• monitor online anti-malware solutions using Office 365 ATP Reports

• perform tests using Attack Simulator

Implement and manage information protection (15-20%)

Secure data access within Office 365

• plan 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 Azure information Protection (AIP)

• plan an AIP solution

• activate Azure Rights Management

• configure usage rights

- configure and manage super users
- customize policy settings
- create and configure labels and conditions
- create and configure templates
- configure languages
- configure and use the AIP scanner

- deploy the RMS connector
- manage tenant keys
- deploy the AIP client
- track and revoke protected documents
- integrate AIP with Microsoft Online Services

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
- create queries to locate sensitive data

Implement and manage Microsoft Cloud App Security

- plan Cloud App Security implementation
- configure Microsoft Cloud App Security
- perform productivity app discovery using Cloud App Security
- manage entries in the Cloud app catalog
- manage third-party apps in Cloud App Security
- manage Microsoft Cloud App Security
- configure Cloud App Security connectors
- configure Cloud App Security policies
- configure and manage Cloud App Security templates
- configure Cloud App Security users and permissions
- review and respond to Cloud App Security alerts
- review and interpret Cloud App Security dashboards and reports
- review and interpret Cloud App Security activity log and governance log

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

Configure and analyze security reporting

- interpret Windows Analytics
- configure Windows Telemetry options
- configure Office Telemetry options
- review and interpret security reports and dashboards
- plan for custom security reporting with Intelligent Security Graph

review Office 365 secure score action and recommendations

• configure reports and dashboards in Azure Log Analytics

• review and interpret reports and dashboards in Azure Log Analytics

• configure alert policies in the Office 365 Security and Compliance Center

Manage and analyze audit logs and reports

• plan for auditing and reporting

• configure Office 365 auditing and reporting

• perform audit log search

• review and interpret compliance reports and dashboards

• configure audit alert policy

Configure Office 365 classification and labeling

• plan for data governance classification and labels

• search for personal data

• apply labels to personal data

• monitor for leaks of personal data

• create and publish Office 365 labels

• configure label policies

Manage data governance and retention

• plan for data governance and retention

• review and interpret data governance reports and dashboards

• configure retention policies

• define data governance event types

• define data governance supervision policies

• configure Information holds

• find and recover deleted Office 365 data

• import data in the Security and Compliance Center

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