Exam MS-101: Microsoft 365 Mobility and Security –

Skills Measured

Implement modern device services (30-35%)

Implement Mobile Device Management (MDM)
- plan for MDM
- configure MDM integration with Azure AD
- set an MDM authority
- set device enrollment limit for users

Manage device compliance
- plan for device Compliance
- design Conditional Access Policies
- create Conditional Access Policies
- configure device compliance policy
- manage Conditional Access Policies

Plan for devices and apps
- create and configure Microsoft Store for Business
- plan app deployment
- plan device co-management
- plan device monitoring
- plan for device profiles
- plan for Mobile Application Management
- plan mobile device security

Plan Windows 10 deployment
- plan for Windows as a Service (WaaS)
- plan the appropriate Windows 10 Enterprise deployment method

- analyze upgrade readiness for Windows 10
- evaluate and deploy additional Windows 10 Enterprise security features

Implement Microsoft 365 security and threat management (30-35%)
Implement Cloud App Security (CAS)
- configure Cloud App Security (CAS)
- configure Cloud App Security (CAS) policies
- configure Connected apps
- design Cloud App Security (CAS) Solution
- manage Cloud App Security (CAS) alerts
- upload cloud app security (CAS) traffic logs

Implement threat management
- plan a threat management solution
- design Azure Advanced Threat Protection (ATP) implementation
- design Microsoft 365 ATP Policies
- configure Azure ATP
- configure Microsoft 365 ATP Policies
- monitor Advanced Threat Analytics (ATA) incidents

Implement Windows Defender Advanced Threat Protection (ATP)
- plan Windows Defender ATP Solution
- configure preferences
- implement Windows Defender ATP Policies
- enable and configure security features of Windows 10 Enterprise

Manage security reports and alerts
- manage service assurance dashboard

- manage tracing and reporting on Azure AD Identity Protection
- configure and manage Microsoft 365 security alerts
- configure and manage Azure Identity Protection dashboard and alerts

Manage Microsoft 365 governance and compliance (35-40%)

Configure Data Loss Prevention (DLP)

- configure DLP Policies
- design data retention policies in Microsoft 365
- manage DLP exceptions
- monitor DLP policy matches
- manage DLP policy matches

Implement Azure Information Protection (AIP)

- plan AIP solution
- plan for deployment On-Prem rights management Connector
- plan for Windows information Protection (WIP) implementation
- plan for classification labeling
- configure Information Rights Management (IRM) for Workloads
- configure Super User
- deploy AIP Clients
- implement Azure Information Protection policies
- implement AIP tenant key

Manage data governance

- configure information retention
- plan for Microsoft 365 backup
- plan for restoring deleted content

- plan information Retention Policies

Manage auditing
- configure audit log retention
- configure audit policy
- monitor Unified Audit Logs

Manage eDiscovery
- search content by using Security and Compliance Center
- plan for in-place and legal hold
- configure eDiscovery and create cases