Exam MS-101: Microsoft 365 Mobility and Security

(**Part of the requirements for:** [Microsoft 365 Certified: Enterprise Administrator Expert](#))

Skills Measured:

Candidates for this exam are Microsoft 365 Enterprise Administrators who take part in evaluating, planning, migrating, deploying, and managing Microsoft 365 services. They perform Microsoft 365 tenant management tasks for an enterprise, including its identities, security, compliance, and supporting technologies.

Implement Modern Device Services (40-45%)

Plan device management

- plan device monitoring
- plan Microsoft Endpoint Manager implementation
- plan for configuration profiles

Manage device compliance

- plan for device compliance
- plan for attack surface reduction
- configure security baselines
- configure device compliance policy

Plan for apps

- create and configure Microsoft Store for Business
- plan app deployment
- plan for mobile application management (MAM)

Plan Windows 10 deployment

- plan for Windows as a Service (Waas)
- plan Windows 10 Enterprise deployment method
- analyze upgrade readiness for Windows 10 by using services such as Desktop Analytics
- evaluate and deploy additional Windows 10 Enterprise security features

Enroll devices

- plan for device join to Azure Active Directory (Azure AD)
- plan for device enrollment

Implement Microsoft 365 Security and Threat Management (20-25%)

Manage security reports and alerts

- evaluate and manage Microsoft Office 365 tenant security by using Secure Score
- manage incident investigation
- review and manage Microsoft 365 security alerts
- manage and review Office 365 security alerts

Plan and implement threat protection with Microsoft Defender

- plan Microsoft Defender for Endpoint
- design Microsoft Defender for Office 365 policies
- implement Microsoft Defender for Identity

Plan Microsoft Cloud App Security

- plan information protection by using Cloud App Security
- plan policies to manage access to cloud apps
- plan for application connectors
- configure Cloud App Security policies
- review and respond to Cloud App Security alerts
- monitor for unauthorized cloud applications

Manage Microsoft 365 Governance and Compliance (35-40%)

Plan for compliance requirements

- plan compliance solutions
- assess compliance
- plan for legislative and regional or industry requirements and drive implementation

Manage information governance

- plan data classification
- plan for classification labeling
- plan for restoring deleted content
- implement records management
- design data retention policies in Microsoft 365

Implement Information protection

- plan information protection solution
- plan and implement label policies
- monitor label alerts and analytics
- deploy Azure Information Protection unified labels clients
- configure Information Rights

Management (IRM) for workloads

- plan for Windows information Protection (WIP) implementation

Plan and implement data loss prevention (DLP)

- plan for DLP
- configure DLP policies
- monitor DLP

Manage search and investigation

- plan for auditing
- plan for eDiscovery
- implement insider risk management
- design Content Search solution