Microsoft 365 Certified: Enterprise Administrator Expert – Skills Measured

Design and implement Microsoft 365 services

Manage domains

- add and configure additional domains
- configure user identities for new domain name
- configure workloads for new domain name
- design domain name configuration
- set primary domain name
- verify custom domain

Plan a Microsoft 365 implementation

- plan for Microsoft 365 on-premises Infrastructure
- plan identity and authentication solution

Setup Microsoft 365 tenancy and subscription

- configure subscription and tenant roles and workload settings
- evaluate Microsoft 365 for organization
- plan and create tenant
- upgrade existing subscriptions to Microsoft 365
- monitor license allocations

Manage Microsoft 365 subscription and tenant health

- manage service health alerts
- create & manage service requests
- create internal service health response plan
- monitor service health
- configure and review reports, including BI, OMS, and Microsoft 365 reporting
- schedule and review security and compliance reports
- schedule and review usage metrics

Plan migration of users and data

- identify data to be migrated and method
- identify users and mailboxes to be migrated and method

- plan migration of on-prem users and groups
- import PST Files

Manage user identity and roles

Design identity strategy

- evaluate requirements and solution for synchronization
- evaluate requirements and solution for identity management
- evaluate requirements and solution for authentication

Plan identity synchronization by using Azure AD Connect

- design directory synchronization
- implement directory synchronization with directory services, federation services, and Azure endpoints

Manage identity synchronization by using Azure AD Connect

- monitor Azure AD Connect Health
- manage Azure AD Connect synchronization
- configure object filters
- configure password sync
- implement multi-forest AD Connect scenarios

Manage Azure AD identities

- plan Azure AD identities
- implement and manage Azure AD self-service password reset
- manage access reviews
- manage groups
- manage passwords
- manage product licenses
- manage users
- perform bulk user management

Manage user roles

- plan user roles
- allocate roles in workloads
- configure administrative accounts
- configure RBAC within Azure AD
- delegate admin rights

- manage admin roles
- manage role allocations by using Azure AD
- plan security and compliance roles for Microsoft 365

Manage access and authentication

Manage authentication

- design authentication method
- configure authentication
- implement authentication method
- manage authentication
- monitor authentication

Implement Multi-Factor Authentication (MFA)

- design an MFA solution
- configure MFA for apps or users
- administer MFA users
- report MFA utilization

Configure application access

- configure application registration in Azure AD
- configure Azure AD application proxy
- publish enterprise apps in Azure AD

Implement access for external users of Microsoft 365 workloads

- create B2B accounts
- create guest accounts
- design solutions for external access

Plan Office 365 workloads and applications

Plan for Office 365 workload deployment

- identify hybrid requirements
- plan connectivity and data flow for each workload
- plan for Microsoft 365 workload connectivity
- plan migration strategy for workloads

Plan Office 365 applications deployment

- manage Office 365 software downloads
- plan for Office 365 apps
- plan for Office 365 Pro plus apps updates
- plan for Office 365 Pro plus connectivity
- plan for Office online
- plan Office 365 Pro plus deployment

Implement modern device services

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

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

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