AZ-500 MICROSOFT AZURE SECURITY TECHNOLOGIES SYLLABUS

Section 1: Manage identities in Azure AD

- Secure users in Azure AD
- Secure directory groups in Azure AD
- Recommend when to use external identities
- Secure external identities
- Implement Azure AD Identity Protection

Section 2: Manage authentication by using Azure AD

- Configure Microsoft Entra Verified ID
- Implementation of multi-factor authentication (MFA)
- Implementation of passwordless authentication
- Implementation of password protection
- Implementation of single sign-on (SSO)
- Integrate single sign-on (SSO) and identity providers
- Recommend and enforce modern authentication protocols

Section 3: Manage authorization by using Azure AD

- Configure Azure role permissions for management groups, subscriptions, resource groups, and resources
- Assign built-in roles in Azure AD
- Assign built-in roles in Azure
- Create and assign custom roles, including Azure roles and Azure AD roles
- Implement and manage Microsoft Entra Permissions Management
- Configure Azure AD Privileged Identity Management (PIM)
- Configure role management and access reviews by using Microsoft Entra Identity Governance
- Implementation of Conditional Access policies

Section 4: Manage application access in Azure AD

- Manage access to enterprise applications in Azure AD, including OAuth permission grants
- Manage app registrations in Azure AD
- Configure app registration permission scopes

- Manage app registration permission consent
- Manage and use service principals
- Manage managed identities for Azure resources
- Recommend when to use and configure an Azure AD Application Proxy, including authentication

Section 5:Plan and implement security for virtual networks

- Plan and implementation of Network Security Groups (NSGs) and Application Security Groups (ASGs)
- Plan and implementation of user-defined routes (UDRs)
- Plan and implementation of VNET peering or VPN gateway
- Plan and implementation of Virtual WAN, including secured virtual hub
- Secure VPN connectivity, including point-to-site and site-to-site
- Implementation of encryption over ExpressRoute
- Configuration of firewall settings on PaaS resources
- Monitor network security by using Network Watcher, including NSG flow logging

Section 6: Plan and implement security for private access to Azure resources

- Plan and implementation of virtual network Service Endpoints
- Plan and implementation of Private Endpoints
- Plan and implementation of Private Link services
- Plan and implement of network integration for Azure App Service and Azure Functions
- Plan and implement of network security configurations for an App Service Environment (ASE)
- Plan and implementation of network security configurations for an Azure SQL Managed Instance

Section 7:Plan and implement security for public access to Azure resources

- Plan and implement TLS to applications, including Azure App Service and API Management
- Plan, implement, and manage an Azure Firewall, including Azure Firewall Manager and firewall policies
- Plan and implementation of an Azure Application Gateway
- Plan and implementation of an Azure Front Door, including a Content Delivery Network (CDN)

- Plan and implementation of a Web Application Firewall (WAF)
- Recommend when to use Azure DDoS Protection Standard

Section 8: Plan and implement advanced security for compute

- Plan and implement remote access to public endpoints, including Azure Bastion and JIT
- Configure network isolation for Azure Kubernetes Service (AKS)
- Secure and monitor AKS
- Configure authentication for AKS
- Configure security monitoring for Azure Container Instances (ACIs)
- Configure security monitoring for Azure Container Apps (ACAs)
- Manage access to Azure Container Registry (ACR)
- Configure disk encryption, including Azure Disk Encryption (ADE), encryption as host, and confidential disk encryption
- Recommend security configurations for Azure API Management

Section 9:Plan and implement security for storage

- Configure access control for storage accounts
- Manage life cycle for storage account access keys
- Select and configure an appropriate method for access to Azure Files
- Select and configure an appropriate method for access to Azure Blob Storage
- Select and configure an appropriate method for access to Azure Tables
- Select and configure an appropriate method for access to Azure Queues
- Select and configure appropriate methods for protecting against data security threats, including soft delete, backups, versioning, and immutable storage
- Configure Bring your own key (BYOK)
- Enable double encryption at the Azure Storage infrastructure level

Section 10:Plan and implement security for Azure SQL Database and Azure SQL Managed Instance

- Enable database authentication by using Microsoft Azure AD
- Enable database auditing
- Identify use cases for the Microsoft Purview governance portal
- Implement data classification of sensitive information by using the Microsoft Purview governance portal

- Plan and implement dynamic masking
- Implementation of Transparent Database Encryption (TDE)
- Recommend when to use Azure SQL Database Always Encrypted

Section 11:Plan, implement, and manage governance for security

- Create, assign, and interpret security policies and initiatives in Azure Policy
- Configure security settings by using Azure Blueprint
- Deploy secure infrastructures by using a landing zone
- Create and configure an Azure Key Vault
- Recommend when to use a Dedicated HSM
- Configure access to Key Vault, including vault access policies and Azure Role Based Access Control
- Manage certificates, secrets, and keys
- Configure key rotation
- Configure backup and recovery of certificates, secrets, and keys

Section 12:Manage security posture by using Microsoft Defender for Cloud

- Identify and remediate security risks by using the Microsoft Defender for Cloud Secure Score and Inventory
- Assess compliance against security frameworks and Microsoft Defender for Cloud
- Add industry and regulatory standards to Microsoft Defender for Cloud
- Add custom initiatives to Microsoft Defender for Cloud
- Connect hybrid cloud and multi-cloud environments to Microsoft Defender for Cloud
- Identify and monitor external assets by using Microsoft Defender External Attack Surface Management
- Configure Microsoft Defender for Servers
- Configure Microsoft Defender for Azure SQL Database
- Manage and respond to security alerts in Microsoft Defender for Cloud
- Configure workflow automation by using Microsoft Defender for Cloud
- Evaluate vulnerability scans from Microsoft Defender for Server

Section 13:Configure and manage security monitoring and automation solutions

- Monitor security events by using Azure Monitor

- Configure data connectors in Microsoft Sentinel
- Create and customize analytics rules in Microsoft Sentinel
- Evaluate alerts and incidents in Microsoft Sentinel
- Configure automation in Microsoft Sentinel