Study guide for Exam AZ-500: Microsoft Azure Security Technologies

Purpose of this document

This study guide should help you understand what to expect on the exam and includes a summary of the topics the exam might cover and links to additional resources. The information and materials in this document should help you focus your studies as you prepare for the exam.

Useful links	Description
Review the skills measured as of May 2, 2023	This list represents the skills measured AFTER the date provided. Study this list if you plan to take the exam AFTER that date.
Review the skills measured prior to May 2, 2023	Study this list of skills if you take your exam PRIOR to the date provided.
Change log	You can go directly to the change log if you want to see the changes that will be made on the date provided.
How to earn the certification	Some certifications only require passing one exam, while others require passing multiple exams.
Certification renewal	Microsoft associate, expert, and specialty certifications expire annually. You can renew by passing a **free** online assessment on Microsoft Learn.
Your Microsoft Learn profile	Connecting your certification profile to Microsoft Learn allows you to schedule and renew exams and share and print certificates.
Exam scoring and score reports	A score of 700 or greater is required to pass.
Exam sandbox	You can explore the exam environment by visiting our exam sandbox.
Request accommodations	If you use assistive devices, require extra time, or need modification to any part of the exam experience, you can request an accommodation.

Useful links	Description
Take a practice test	Are you ready to take the exam or do you need to study a bit more?

Updates to the exam

Our exams are updated periodically to reflect skills that are required to perform a role. We have included two versions of the Skills Measured objectives depending on when you are taking the exam.

We always update the English language version of the exam first. Some exams are localized into other languages, and those are updated approximately eight weeks after the English version is updated. While Microsoft makes every effort to update localized versions as noted, there may be times when the localized versions of an exam are not updated on this schedule. Other available languages are listed in the **Schedule Exam** section of the **Exam Details** webpage. If the exam isn't available in your preferred language, you can request an additional 30 minutes to complete the exam.

Note

The bullets that follow each of the skills measured are intended to illustrate how we are assessing that skill. Related topics may be covered in the exam.

Note

Most questions cover features that are general availability (GA). The exam may contain questions on Preview features if those features are commonly used.

Skills measured as of May 2, 2023

Audience profile

The Azure Security Engineer implements, manages, and monitors security for resources in Azure, multi-cloud, and hybrid environments as part of an end-to-end infrastructure. They recommend security components and configurations to protect identity & access, data, applications, and networks.

Responsibilities for an Azure Security Engineer include managing the security posture, identifying and remediating vulnerabilities, performing threat modelling, and implementing threat protection. They may also participate in responding to security incidents.

Azure Security Engineers work with architects, administrators, and developers to plan and implement solutions that meet security and compliance requirements.

The Azure Security Engineer should have practical experience in administration of Microsoft Azure and hybrid environments. The Azure Security Engineer should have a strong familiarity with compute, network, and storage in Azure, as well as Azure Active Directory, part of Microsoft Entra.

- Manage identity and access (25–30%)
- Secure networking (20–25%)
- Secure compute, storage, and databases (20–25%)

- Manage security operations (25–30%)

Manage identity and access (25–30%)

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

Manage authentication by using Azure AD

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

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
- Implement Conditional Access policies

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

Secure networking (20–25%)

Plan and implement security for virtual networks

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

Plan and implement security for private access to Azure resources

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

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 implement an Azure Application Gateway
- Plan and implement an Azure Front Door, including Content Delivery Network (CDN)
- Plan and implement a Web Application Firewall (WAF)
- Recommend when to use Azure DDoS Protection Standard

Secure compute, storage, and databases (20–25%)

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

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

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
- Implement Transparent Database Encryption (TDE)
- Recommend when to use Azure SQL Database Always Encrypted

Manage security operations (25–30%)

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

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 and manage threat protection by using Microsoft Defender for Cloud

- Enable workload protection services in Microsoft Defender for Cloud, including Microsoft Defender for Storage, Databases, Containers, App Service, Key Vault, Resource Manager, and DNS
- 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

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

Study resources

We recommend that you train and get hands-on experience before you take the exam. We offer self-study options and classroom training as well as links to documentation, community sites, and videos.

Study resources	Links to learning and documentation
Get trained	Choose from self-paced learning paths and modules or take an instructor-led course
Find documentation	Azure documentation Azure Active Directory (AD)

Study resources	Links to learning and documentation
	Azure Firewall documentation Azure Firewall Manager documentation Azure Application Gateway documentation Azure Front Door and CDN Documentation Web Application Firewall documentation Azure Key Vault documentation Azure virtual network service endpoint policies Manage Azure Private Endpoints - Azure Private Link Create a Private Link service by using the Azure portal Azure DDoS Protection Standard documentation Endpoint Protection on a Windows VM in Azure Secure and use policies - Azure Virtual Machines Security - Azure App Service Azure Policy documentation Overview of Microsoft Defender for Servers Microsoft Defender for Cloud documentation Microsoft Threat Modeling Tool overview Azure Monitor documentation Microsoft Sentinel documentation Azure Storage documentation Azure Files documentation Azure SQL documentation
Ask a question	Microsoft Q&A | Microsoft Docs
Get community support	Azure Community Support
Follow Microsoft Learn	Microsoft Learn - Microsoft Tech Community
Find a video	Exam Readiness Zone Azure Fridays Browse other Microsoft Learn shows

Change log

Key to understanding the table: The topic groups (also known as functional groups) are in bold typeface followed by the objectives within each group. The table is a comparison between the two versions of the exam skills measured and the third column describes the extent of the changes.

Skill area prior to May 2, 2023	Skill area as of May 2, 2023	Changes
Audience profile		No change
Manage identity and access	**Manage identity and access**	No change
Manage identities in Azure AD	Manage identities in Azure AD	No change
Manage authentication by using Azure AD	Manage authentication by using Azure AD	No change
Manage authorization by using Azure AD	Manage authorization by using Azure AD	No change
Manage application access in Azure AD	Manage application access in Azure AD	Minor
Secure networking	**Secure networking**	No change
Plan and implement security for virtual networks	Plan and implement security for virtual networks	No change
Plan and implement security for private access to Azure resources	Plan and implement security for private access to Azure resources	No change
Plan and implement security for public access to Azure resources	Plan and implement security for public access to Azure resources	No change
Secure compute, storage, and databases	**Secure compute, storage, and databases**	No change
Plan and implement advanced security for compute	Plan and implement advanced security for compute	No change
Plan and implement security for storage	Plan and implement security for storage	No change
Plan and implement security for Azure SQL Database and Azure SQL Managed Instance	Plan and implement security for Azure SQL Database and Azure SQL Managed Instance	Minor
Manage security operations	**Manage security operations**	No change
Plan, implement, and manage governance for security	Plan, implement, and manage governance for security	No change

Skill area prior to May 2, 2023	Skill area as of May 2, 2023	Changes
Manage security posture by using Microsoft Defender for Cloud	Manage security posture by using Microsoft Defender for Cloud	No change
Configure and manage threat protection by using Microsoft Defender for Cloud	Configure and manage threat protection by using Microsoft Defender for Cloud	No change
Configure and manage security monitoring and automation solutions	Configure and manage security monitoring and automation solutions	No change

Skills measured prior to May 2, 2023

Audience profile

The Azure Security Engineer implements, manages, and monitors security for resources in Azure, multi-cloud, and hybrid environments as part of an end-to-end infrastructure. They recommend security components and configurations to protect identity & access, data, applications, and networks.

Responsibilities for an Azure Security Engineer include managing the security posture, identifying and remediating vulnerabilities, performing threat modelling, and implementing threat protection. They may also participate in responding to security incidents.

Azure Security Engineers work with architects, administrators, and developers to plan and implement solutions that meet security and compliance requirements.

The Azure Security Engineer should have practical experience in administration of Microsoft Azure and hybrid environments. The Azure Security Engineer should have a strong familiarity with compute, network, and storage in Azure, as well as Azure Active Directory, part of Microsoft Entra.

- Manage identity and access (25–30%)
- Secure networking (20–25%)
- Secure compute, storage, and databases (20–25%)
- Manage security operations (25–30%)

Manage identity and access (25–30%)

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

Manage authentication by using Azure AD

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

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
- Implement Conditional Access policies

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 authentication for an Azure AD Application Proxy

Secure networking (20–25%)

Plan and implement security for virtual networks

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

Plan and implement security for private access to Azure resources

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

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 implement an Azure Application Gateway
- Plan and implement an Azure Front Door, including Content Delivery Network (CDN)
- Plan and implement a Web Application Firewall (WAF)
- Recommend when to use Azure DDoS Protection Standard

Secure compute, storage, and databases (20–25%)

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

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

Plan and implement security for Azure SQL Database and Azure SQL Managed Instance

- Enable database authentication by using Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra
- 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
- Implement Transparent Database Encryption (TDE)
- Recommend when to use Azure SQL Database Always Encrypted

Manage security operations (25–30%)

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

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 and manage threat protection by using Microsoft Defender for Cloud

- Enable workload protection services in Microsoft Defender for Cloud, including Microsoft Defender for Storage, Databases, Containers, App Service, Key Vault, Resource Manager, and DNS
- 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

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