AZ-500T00 Microsoft Azure Security Technologies

Category: Networking & Security | **Vendor:** Microsoft

Duration: 32.00 hours (4 days) **26.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format:	Instructor Led - Online
Certification:	Microsoft Certified: Azure Security Engineer Associate
Related Exam:	AZ-500

Course Overview

This course provides IT Security Professionals with the knowledge and skills needed to implement security controls, maintain an organization's security posture, and identify and remediate security vulnerabilities. This course includes security for identity and access, platform protection, data and applications, and security operations.

About This Course

This course provides IT Security Professionals with the knowledge and skills needed to implement security controls, maintain an organization's security posture, and identify and remediate security vulnerabilities. This course includes security for identity and access, platform protection, data and applications, and security operations.

Who Should Attend

This course is for Azure Security Engineers who are planning to take the associated certification exam, or who are performing security tasks in their day-to-day job. This course would also be helpful to an engineer that wants to specialize in providing security for Azure-based digital platforms and play an integral role in protecting an organization's data.

Prerequisites & Entry Requirements

General Prerequisites:

- AZ-104T00 - Microsoft Azure Administrator
- Security best practices and industry security requirements such as defense in depth, least privileged access, role-based access control, multi-factor authentication, shared responsibility, and zero trust model.
- Be familiar with security protocols such as Virtual Private Networks (VPN), Internet Security Protocol (IPSec), Secure Socket Layer (SSL), disk and data encryption methods.
- Have some experience deploying Azure workloads. This course does not cover the basics of Azure administration, instead the course content builds on that knowledge by adding security specific information.
- Have experience with Windows and Linux operating systems and scripting languages. Course labs may use PowerShell and the CLI.

Detailed Course Outline

1 - Manage identities in Microsoft Entra ID

- Secure users in Microsoft Entra ID
- Secure groups in Microsoft Entra ID
- Recommend when to use external identities
- Secure external identities
- Implement Microsoft Entra Identity protection

2 - Manage authentication by using Microsoft Entra ID

- Configure Microsoft Entra Verified ID
- Implement multifactor 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

3 - Manage authorization by using Microsoft Entra ID

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

4 - Manage application access in Microsoft Entra ID

- Manage access to enterprise applications in Microsoft Entra ID, including OAuth permission grants
- Manage app registrations in Microsoft Entra ID
- 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 a Microsoft Entra Application Proxy, including authentication

5 - 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 Virtual Network peering or gateway
- Plan and implement Virtual Wide Area Network, 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

6 - 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

7 - Plan and implement security for public access to Azure resources

- Plan and implement Transport Layer Security (TLS) to applications, including Azure App Service and API Management
- Plan, implement, and manage an Azure Firewall, 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

8 - Plan and implement advanced security for compute

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

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

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

- Enable database authentication by using Microsoft Entra ID
- Enable and monitor database audit
- 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 mask
- Implement transparent data encryption
- Recommend when to use Azure SQL Database Always Encrypted

11 - Plan, 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 Hardware Security Module (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, and keys

12 - Manage security posture by using Microsoft Defender for Cloud

- Implement 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 multicloud environments to Microsoft Defender for Cloud
- Identify and monitor external assets by using Microsoft Defender External Attack Surface Management

13 - 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

14 - 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
- Configure automation in Microsoft Sentinel

,

1 - Manage security controls for identity and access

- Microsoft cloud security benchmark: Identity management and privileged access
- What is Microsoft Entra ID?
- Secure Microsoft Entra users
- Create a new user in Microsoft Entra ID
- Secure Microsoft Entra groups
- Recommend when to use external identities
- Secure external identities
- Implement Microsoft Entra Identity Protection
- Microsoft Entra Connect
- Microsoft Entra Cloud Sync
- Authentication options
- Password hash synchronization with Microsoft Entra ID
- Microsoft Entra pass-through authentication
- Federation with Microsoft Entra ID
- What is Microsoft Entra authentication?
- Implement multifactor authentication (MFA)
- Kerberos authentication
- New Technology Local Area Network Manager (NTLM)
- Passwordless authentication options for Microsoft Entra ID
- Implement passwordless authentication
- Implement password protection
- Microsoft Entra ID single sign-on
- Implement single sign-on (SSO)
- Integrate single sign-on (SSO) and identity providers
- Configure Microsoft Entra Verified ID
- Recommend and enforce modern authentication protocols
- Azure management groups
- Configure Azure role permissions for management groups, and resources
- Azure role-based access control
- Azure built-in roles
- Assign Azure role permissions for management groups, and resources

Microsoft Entra built-in roles

- Assign built-in roles in Microsoft Entra ID
- Microsoft Entra role-based access control
- Create and assign a custom role in Microsoft Entra ID
- Zero Trust security
- Microsoft Entra Privileged Identity Management
- Configure Privileged Identity Management
- Microsoft Entra ID governance
- Identity lifecycle management
- Lifecycle workflows
- Entitlement management
- Delegation and roles in entitlement management
- Access reviews
- Configure role management and access reviews by using Microsoft Entra ID governance
- Implement Conditional Access policies for Cloud Resources in Azure
- Azure lighthouse overview
- Module assessment

2 - Manage Microsoft Entra application access

- Manage access to enterprise applications in Microsoft Entra ID, including authentication
- Module assessment

3 - Plan and implement security for virtual networks

- Microsoft Cloud Security Benchmark: Data Protection, Logging and Threat Detection, and Network Security
- What is an Azure Virtual Network
- Azure Virtual Network Manager
- Plan and implement Network Security Groups (NSGs) and Application Security Groups (ASGs)
- Plan and implement User-Defined Routes (UDRs)
- Plan and implement Virtual Network peering or gateway
- Plan and implement Virtual Wide Area Network, including point-to-site and site-to-site
- Azure encryption
- What is Azure Virtual Network encryption
- Azure ExpressRoute
- Implement encryption over ExpressRoute
- Configure firewall settings on Azure resources
- Monitor network security by using Network Watcher
- Module assessment

4 - 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
- Module assessment

5 - Plan and implement security for public access to Azure resources

- Plan and implement Transport Layer Security (TLS) to applications, Azure Firewall Manager and firewall policies
- Plan and implement an Azure Application Gateway
- Plan and implement a Web Application Firewall (WAF)
- Plan and implement an Azure Front Door, including Content Delivery Network (CDN)
- Recommend when to use Azure DDoS Protection Standard
- Module assessment

6 - Plan and implement advanced security for compute

- Plan and implement remote access to public endpoints, Azure Bastion and just-in-time (JIT) virtual machine (VM) access
- What is Azure Kubernetes Service?
- Configure network isolation for Azure Kubernetes Service (AKS)
- Secure and monitor Azure Kubernetes Service
- Configure authentication for Azure Kubernetes Service
- Configure security for Azure Container Instances (ACIs)
- Configure security for Azure Container Apps (ACAs)
- Manage access to Azure Container Registry (ACR)
- Configure disk encryption, and confidential disk encryption
- Recommend security configurations for Azure API Management
- Module assessment

7 - Plan and implement security for storage

- Azure 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 Blobs
- 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, and immutable storage
- Configure Bring your own key (BYOK)
- Enable double encryption at the Azure Storage infrastructure level
- Module assessment

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

- Azure SQL Database and SQL Managed Instance security
- Enable Microsoft Entra database authentication
- Enable and monitor database audit
- 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 mask
- Implement transparent data encryption
- Recommend when to use Azure SQL Database Always Encrypted
- Implement an Azure SQL Database firewall
- Module assessment

9 - Implement and manage enforcement of cloud governance policies

- Microsoft cloud security benchmark: Access, Data, Identity, Network, Endpoint, Governance, Recovery, Incident, and Vulnerability Management
- Azure governance
- Create, and interpret security policies and initiatives in Azure Policy
- Deploy secure infrastructures by using a landing zone
- Azure Key Vault
- Azure Key Vault security
- Azure Key Vault authentication
- Create and configure an Azure Key Vault
- Recommend when to use a dedicated Hardware Security Module (HSM)
- Configure access to Key Vault, including vault access policies and Azure role-based access control
- Manage certificates, and keys
- Implement security controls to protect backups
- Implement security controls for asset management
- Module assessment

10 - Manage security posture by using Microsoft Defender for Cloud

- Implement 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 multicloud environments to Microsoft Defender for Cloud
- Implement and use Microsoft Defender External Attack Surface Management
- Module assessment

11 - Configure and manage threat protection by using Microsoft Defender for Cloud

- Enable workload protection services in Microsoft Defender for Cloud
- Defender for Servers
- Defender for Storage
- Malware scanning in Defender for Storage
- Detect threats to sensitive data
- Deploy Microsoft Defender for Storage
- Enable configure Azure built-in policy
- Configure Microsoft Defender plans for Servers, and Storage
- Implement and manage Microsoft Defender Vulnerability Management
- Log Analytics workspace
- Manage data retention in a Log Analytics workspace
- Deploy the Azure Monitor Agent
- Collect data with Azure Monitor Agent
- Data collection rules (DCRs) in Azure Monitor
- Transformations in data collection rules (DCRs)
- Monitor network security events and performance data by configuring data collection rules (DCRs) in Azure Monitor
- Connect your Azure subscriptions
- Just-in-time machine access
- Enable just-in-time access
- Container security in Microsoft Defender for Containers
- Managed Kubernetes threat factors
- Defender for Containers architecture
- Configure Microsoft Defender for Containers components
- Microsoft Defender for Cloud DevOps Security
- DevOps Security support and prerequisites
- DevOps environment security posture
- Connect your GitHub lab environment to Microsoft Defender for Cloud
- Configure the Microsoft Security DevOps GitHub action
- Defender for Cloud AI threat protection
- Enable threat protection for AI workloads in Defender for Cloud

Gain application and end-user context for AI alerts

12 - Configure and manage security monitoring and automation solutions

- Manage and respond to security alerts in Microsoft Defender for Cloud
- Configure workflow automation by using Microsoft Defender for Cloud
- Log retention plans in Microsoft Sentinel
- Alerts and Incidents from Microsoft Sentinel
- Configure data connectors in Microsoft Sentinel
- Enable analytics rules in Microsoft Sentinel
- Configure automation in Microsoft Sentinel
- Automating Threat Response with Microsoft Sentinel
- Module assessment

□□ Certification Path

Microsoft Certified: Azure Security Engineer Associate

Exam: AZ-500

Upcoming Schedule

Available training dates for AZ-500T00 Microsoft Azure Security Technologies:

Start Date	End Date	Location	Delivery	Price
12 Oct 2026	15 Oct 2026	Online	Virtual	€2,495.00
16 Nov 2026	19 Nov 2026	Online	Virtual	€2,495.00
18 Jan 2027	21 Jan 2027	Online	Virtual	€2,495.00

Additional Course Details

Nexus Humans AZ-500 Microsoft Azure Security Technologies training program is a workshop that presents an invigorating mix of sessions, lessons, and masterclasses meticulously crafted to propel your learning expedition forward.

This immersive bootcamp-style experience boasts interactive lectures, hands-on labs, and collaborative hackathons, all strategically designed to fortify fundamental concepts.

Guided by seasoned coaches, each session offers priceless insights and practical skills crucial for honing your expertise. Whether you're stepping into the realm of professional skills or a seasoned professional, this comprehensive course ensures you're equipped with the knowledge and prowess necessary for success.

While we feel this is the best course for the AZ-500 Microsoft Azure Security Technologies course and one of our Top 10 we encourage you to read the course outline to make sure it is the right content for you.

Additionally, private sessions, closed classes or dedicated events are available both live online and at our training centres in Dublin and London, as well as at your offices anywhere in the UK, Ireland or across EMEA.

Frequently Asked Questions

Q: What delivery options are available for AZ-500T00 Microsoft Azure Security Technologies?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The AZ-500T00 Microsoft Azure Security Technologies course helps prepare you for the Microsoft Certified: Azure Security Engineer Associate certification path.

Q: Which exam does this course prepare me for?

This course prepares you for the AZ-500 official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

Q: How many CPD hours does this course provide?

The 4-day AZ-500T00 Microsoft Azure Security Technologies course provides up to 26.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the AZ-500T00 Microsoft Azure Security Technologies training?

The training takes place over 4 day(s), with each day lasting approximately 32.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for AZ-500T00 Microsoft Azure Security Technologies?

Yes, we provide corporate training, dedicated training, and closed classes for AZ-500T00 Microsoft Azure Security Technologies. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: az500 az 500, AZ-500T00: Secure cloud resources with Microsoft security technologies, Microsoft, vILT, AZ-500T00

Q: Why choose Nexus Human for AZ-500T00 Microsoft Azure Security Technologies?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your AZ-500T00 Microsoft Azure Security Technologies training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)