

# Microsoft Cloud Computing & Security

---

*In this comprehensive course, you will gain a deep understanding of how to secure user access to your organization's Microsoft 365 resources utilizing the powerful features of Microsoft Entra ID, Microsoft Defender, and Microsoft Purview. The course begins with an in-depth exploration of user password protection strategies, multi-factor authentication, Identity Protection, Microsoft Entra Connect, and the implementation of conditional access in Microsoft 365. You will learn to fortify your Microsoft 365 environment against potential threats by studying threat vectors and deploying advanced threat protection technologies such as Secure Score, Exchange Online protection, Microsoft 365 Defender, and robust threat management techniques.*

*Additionally, the course delves into Microsoft Purview's information protection technologies, where you will discover how to manage information rights, apply message encryption, and utilize labels, policies, and rules to support data loss prevention and information protection. Furthermore, the course covers essential topics on archiving and retention within Microsoft 365, focusing on data governance, implementing data retention policies and tags, and managing in-place records for SharePoint and email retention.*

*Lastly, the course equips you with the skills to conduct comprehensive content searches and investigations, including eDiscovery and audit capabilities, ensuring that you can efficiently manage and protect your organization's data. By the end of this course, you will be proficient in leveraging Microsoft 365's security, compliance, and governance features to create a secure and compliant digital workplace.*

## Required Prerequisites

### Course Prerequisites:

- **Fundamental Knowledge of Networking:** Understanding basic networking concepts, including IP addressing, DNS, and VPNs, will be beneficial.
- **Awareness of IT Security Principles:** General knowledge of IT security principles and practices, such as authentication, authorization, and encryption, will help you grasp the course material more effectively.
- **Basic IT Proficiency:** Basic proficiency in IT concepts and practices, such as operating

system management and application software usage, will provide a solid foundation for the course.

## **Table of contents**

### **Module 1: Describe cloud concepts**

Describe cloud computing

- Define cloud computing
- Describe the shared responsibility model
- Define cloud models, including public, private, and hybrid
- Identify appropriate use cases for each cloud model
- Describe the consumption-based model
- Compare cloud pricing models
- Describe serverless

Describe the benefits of using cloud services

- Describe the benefits of high availability and scalability in the cloud
- Describe the benefits of reliability and predictability in the cloud
- Describe the benefits of security and governance in the cloud
- Describe the benefits of manageability in the cloud

Describe cloud service types

- Describe infrastructure as a service (IaaS)
- Describe platform as a service (PaaS)
- Describe software as a service (SaaS)
- Identify appropriate use cases for each cloud service type (IaaS, PaaS, and SaaS)

### **Module 2: Describe Azure architecture and services**

Describe the core architectural components of Azure

- Describe Azure regions, region pairs, and sovereign regions
- Describe availability zones
- Describe Azure datacenters
- Describe Azure resources and resource groups
- Describe subscriptions
- Describe management groups

- Describe the hierarchy of resource groups, subscriptions, and management groups

#### Describe Azure compute and networking services

- Compare compute types, including containers, virtual machines, and functions
- Describe virtual machine options, including Azure virtual machines, Azure Virtual Machine Scale Sets, availability sets, and Azure Virtual Desktop
- Describe the resources required for virtual machines
- Describe application hosting options, including web apps, containers, and virtual machines
- Describe virtual networking, including the purpose of Azure virtual networks, Azure virtual subnets, peering, Azure DNS, Azure VPN Gateway, and ExpressRoute
- Define public and private endpoints

#### Describe Azure storage services

- Compare Azure Storage services
- Describe storage tiers
- Describe redundancy options
- Describe storage account options and storage types
- Identify options for moving files, including AzCopy, Azure Storage Explorer, and Azure File Sync
- Describe migration options, including Azure Migrate and Azure Data Box

#### Describe Azure identity, access, and security

- Describe directory services in Azure, including Microsoft Entra ID and Microsoft Entra Domain Services
- Describe authentication methods in Azure, including single sign-on (SSO), multi-factor authentication (MFA), and passwordless
- Describe external identities in Azure, including business-to-business (B2B) and business-to-customer (B2C)
- Describe Microsoft Entra Conditional Access
- Describe Azure role-based access control (RBAC)
- Describe the concept of Zero Trust
- Describe the purpose of the defense-in-depth model
- Describe the purpose of Microsoft Defender for Cloud

## **Module 3: Describe Azure management and governance**

Describe cost management in Azure

- Describe factors that can affect costs in Azure
- Compare the pricing calculator and the Total Cost of Ownership (TCO) Calculator
- Describe cost management capabilities in Azure
- Describe the purpose of tags

Describe features and tools in Azure for governance and compliance

- Describe the purpose of Microsoft Purview in Azure
- Describe the purpose of Azure Policy
- Describe the purpose of resource locks

Describe features and tools for managing and deploying Azure resources

- Describe the Azure portal
- Describe Azure Cloud Shell, including Azure Command-Line Interface (CLI) and Azure PowerShell
- Describe the purpose of Azure Arc
- Describe infrastructure as code (IaC)
- Describe Azure Resource Manager (ARM) and ARM templates

Describe monitoring tools in Azure

- Describe the purpose of Azure Advisor
- Describe Azure Service Health
- Describe Azure Monitor, including Log Analytics, Azure Monitor alerts, and Application Insights

## **Module 4: Describe the concepts of security, compliance, and identity**

Describe security and compliance concepts

- Describe the shared responsibility model
- Describe defense-in-depth
- Describe the Zero Trust model

- Describe encryption and hashing
- Describe Governance, Risk, and Compliance (GRC) concepts

Define identity concepts

- Define identity as the primary security perimeter
- Define authentication
- Define authorization
- Describe identity providers
- Describe the concept of directory services and Active Directory
- Describe the concept of federation

## **Module 5: Describe the capabilities of Microsoft Entra**

Describe function and identity types of Microsoft Entra ID

- Describe Microsoft Entra ID
- Describe types of identities
- Describe hybrid identity

Describe authentication capabilities of Microsoft Entra ID

- Describe the authentication methods
- Describe multi-factor authentication (MFA)
- Describe password protection and management capabilities

Describe access management capabilities of Microsoft Entra ID

- Describe Conditional Access
- Describe Microsoft Entra roles and role-based access control (RBAC)

Describe identity protection and governance capabilities of Microsoft Entra

- Describe Microsoft Entra ID Governance
- Describe access reviews

- Describe the capabilities of Microsoft Entra Privileged Identity Management
- Describe Microsoft Entra ID Protection
- Describe Microsoft Entra Permissions Management

## **Module 6: Describe the capabilities of Microsoft security solutions**

Describe core infrastructure security services in Azure

- Describe Azure distributed denial-of-service (DDoS) Protection
- Describe Azure Firewall
- Describe Web Application Firewall (WAF)
- Describe network segmentation with Azure virtual networks
- Describe network security groups (NSGs)
- Describe Azure Bastion
- Describe Azure Key Vault

Describe security management capabilities of Azure

- Describe Microsoft Defender for Cloud
- Describe Cloud Security Posture Management (CSPM)
- Describe how security policies and initiatives improve the cloud security posture
- Describe enhanced security features provided by cloud workload protection

Describe capabilities of Microsoft Sentinel

- Define the concepts of security information and event management (SIEM) and security orchestration automated response (SOAR)
- Describe threat detection and mitigation capabilities in Microsoft Sentinel

Describe threat protection with Microsoft Defender XDR

- Describe Microsoft Defender XDR services
- Describe Microsoft Defender for Office 365
- Describe Microsoft Defender for Endpoint

- Describe Microsoft Defender for Cloud Apps
- Describe Microsoft Defender for Identity
- Describe Microsoft Defender Vulnerability Management
- Describe Microsoft Defender Threat Intelligence (Defender TI)
- Describe the Microsoft Defender portal

## **Module 7: Describe the capabilities of Microsoft compliance solutions**

Describe Microsoft Service Trust Portal and privacy principles

- Describe the Service Trust Portal offerings
- Describe the privacy principles of Microsoft
- Describe Microsoft Privacy

Describe compliance management capabilities of Microsoft Purview

- Describe the Microsoft Purview compliance portal
- Describe Compliance Manager
- Describe the uses and benefits of compliance score

Describe information protection, data lifecycle management, and data governance capabilities of Microsoft Purview

- Describe the data classification capabilities
- Describe the benefits of Content explorer and Activity explorer
- Describe sensitivity labels and sensitivity label policies
- Describe data loss prevention (DLP)
- Describe records management
- Describe retention policies, retention labels, and retention label policies
- Describe unified data governance solutions in Microsoft Purview

Describe insider risk, eDiscovery, and audit capabilities in Microsoft Purview

- Describe insider risk management
- Describe eDiscovery solutions in Microsoft Purview
- Describe audit solutions in Microsoft Purview

## **Module 8: Describe Microsoft 365 apps and services**

Describe productivity solutions of Microsoft 365

- Describe the core productivity capabilities and benefits of Microsoft 365 including Microsoft Outlook and Microsoft Exchange, Microsoft 365 apps, and OneDrive
- Describe core Microsoft 365 Apps including Microsoft Word, Excel, PowerPoint, Outlook, and OneNote
- Describe work management capabilities of Microsoft 365 including Microsoft Project, Planner, Bookings, Forms, Lists, and To Do

Describe collaboration solutions of Microsoft 365

- Describe the collaboration benefits and capabilities of Microsoft 365 including Microsoft Exchange, Outlook, SharePoint, OneDrive, and Stream
- Describe the collaboration benefits and capabilities of Microsoft Teams and Teams Phone
- Describe the Microsoft Viva apps
- Describe the ways that you can extend Microsoft Teams by using collaborative apps

## **Module 9: Describe security, compliance, privacy, and trust in Microsoft 365**

Describe identity and access management solutions of Microsoft 365

- Describe the identity and access management capabilities of Microsoft Entra ID
- Describe cloud identity, on-premises identity, and hybrid identity concepts
- Describe how Microsoft uses methods such as multi-factor authentication (MFA), self-service password reset (SSPR), and conditional access, to keep identities, access, and data secure



Describe threat protection solutions of Microsoft 365

- Describe Microsoft Defender XDR, Defender for Endpoint, Defender for Office 365, Defender for Identity, Defender for Cloud Apps, and the Microsoft Defender Portal
- Describe Microsoft Secure Score benefits and capabilities
- Describe how Microsoft 365 addresses the most common types of threats against endpoints, applications, and identities

Describe trust, privacy, risk, and compliance solutions of Microsoft 365

- Describe the Zero Trust Model
- Describe Microsoft Purview compliance solutions such as insider risk, auditing, and eDiscovery
- Describe Microsoft Purview Information Protection features such as sensitivity labels and data loss prevention
- Describe how Microsoft supports data residency to ensure regulatory compliance
- Describe the capabilities and benefits of Microsoft Privacy

## **Module 10: Describe Microsoft 365 pricing, licensing, and support**

Identify Microsoft 365 pricing and billing management options

- Describe the pricing model for Microsoft cloud services including enterprise agreements, cloud solution providers, and direct billing
- Describe available billing and bill management options including billing frequency and methods of payment

Identify licensing options available in Microsoft 365

- Describe license management
- Describe the differences between base licensing and add-on licensing

Identify support options for Microsoft 365 services

- Describe how to create a support request for Microsoft 365 services

- Describe support options for Microsoft 365 services
- Describe service-level agreements (SLAs) including service credits
- Determine service health status by using the Microsoft 365 admin center or the Microsoft Entra admin center