

Introduction to Microsoft Security, Compliance, and Identity

Download Whitepaper: Accelerate Your Modernization Efforts with a Cloud-Native Strategy
Get Your Free Copy Now

Course Number: SC-900T00

Duration: 1 days

Overview

Course Description

This course provides introductory level knowledge on security, compliance, and identity concepts and related cloud-based Microsoft solutions.

Audience Profile

The audience for this course is looking to obtain an introduction to security, compliance, and identity (SCI) across cloud-based and related Microsoft services. The content for this course aligns to the SC-900 exam objective domain. Candidates should be familiar with Microsoft Azure and Microsoft 365 and understand how Microsoft security, compliance, and identity solutions can span across these solution areas to provide a holistic and end-to-end solution. Before attending this course, students must have:

- General understanding of networking and cloud computing concepts.
- General IT knowledge or any general experience working in an IT environment.
- General understanding of Microsoft Azure and Microsoft 365.

Skills Gained

After completing this course, students will be able to:

- Describe basic concepts of security, compliance, and identity.
- Describe the concepts and capabilities of Microsoft identity and access management solutions.
- Describe the capabilities of Microsoft security solutions.
- Describe the compliance management capabilities in Microsoft.

Prerequisites

Before attending this course, students must have:

- General understanding of networking and cloud computing concepts.
- General IT knowledge or any general experience working in an IT environment.
- General understanding of Microsoft Azure and Microsoft 365.

Audience

Course Details

Outline

- 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
 - Module assessment
 - Summary and resources
- Describe identity concepts
 - Define authentication and authorization
 - Define identity as the primary security perimeter
 - Describe the role of the identity provider
 - Describe the concept of directory services and Active Directory
 - Describe the concept of federation
 - Module assessment

- Summary and resources
- Describe the function and identity types of Microsoft Entra ID
 - Describe Microsoft Entra
 - Describe Microsoft Entra ID
 - Describe types of identities
 - Describe Microsoft Entra Agent ID
 - Describe hybrid identity
 - Describe external identities
 - Module assessment
 - Summary & resources
- Describe the authentication capabilities of Microsoft Entra ID
 - Describe authentication methods
 - Describe multifactor authentication
 - Describe self-service password reset
 - Describe password protection and management capabilities
 - Module assessment
 - Summary and resources
- Describe access management capabilities of Microsoft Entra
 - Describe Conditional Access
 - Describe Global Secure Access in Microsoft Entra
 - Describe Microsoft Entra roles and role-based access control (RBAC)
 - Module assessment
 - Summary & resources
- Describe the identity protection and governance capabilities of Microsoft Entra
 - Describe Microsoft Entra ID Governance
 - Describe access reviews
 - Describe entitlement management
 - Describe the capabilities of Privileged Identity Management
 - Describe Microsoft Entra ID Protection
 - Describe Microsoft Entra Verified ID
 - Describe Microsoft Entra integration with Microsoft Security Copilot
 - Module assessment

- Summary & resources
- Describe Microsoft Security Copilot
 - Get acquainted with Microsoft Security Copilot
 - Describe Microsoft Security Copilot terminology
 - Describe how Microsoft Security Copilot processes prompt requests
 - Describe the elements of an effective prompt
 - Describe how to enable Microsoft Security Copilot
 - Module assessment
 - Summary and resources
- Describe core infrastructure security services in Azure
 - Describe Azure DDoS protection
 - Describe Azure Firewall
 - Describe Web Application Firewall
 - Describe network segmentation in Azure
 - Describe Azure Network Security Groups
 - Describe Azure Bastion
 - Describe Azure Key Vault
 - Module assessment
 - Summary and resources
- Describe the security management capabilities in Azure
 - Describe Microsoft Defender for Cloud
 - Describe how security policies, standards, and recommendations improve cloud security posture
 - Describe Cloud security posture management
 - Describe the enhanced security of Microsoft Defender for Cloud
 - Describe DevOps security management
 - Module assessment
 - Summary and resources
- Describe security capabilities of Microsoft Sentinel
 - Define the concepts of SIEM and SOAR
 - Describe threat detection and mitigation capabilities in Microsoft Sentinel
 - Describe Microsoft Sentinel integration with Microsoft Security Copilot

- Module assessment
- Summary and resources
- 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
 - Describe Microsoft Security Exposure Management
 - Describe the Microsoft Defender portal
 - Describe Copilot integration with Microsoft Defender XDR
 - Module assessment
 - Summary and resources
- Describe Microsoft's Service Trust portal and privacy principles
 - Describe the offerings of the Service Trust portal
 - Describe Microsoft's privacy principles
 - Module assessment
 - Summary and resources
- Describe the data security solutions of Microsoft Purview
 - Describe the data classification capabilities of Microsoft Purview Information Protection
 - Describe sensitivity labels and policies in Microsoft Purview Information Protection
 - Describe data loss prevention in Microsoft Purview
 - Describe insider risk management in Microsoft Purview
 - Describe adaptive protection in Microsoft Purview
 - Describe Data Security Posture Management
 - Describe Microsoft Purview Data Security Investigations
 - Module assessment
- Describe the data compliance solutions of Microsoft Purview
 - Describe Compliance Manager

- Describe Communication Compliance
- Describe eDiscovery
- Describe audit in Microsoft Purview
- Describe Data Lifecycle Management
- Describe Microsoft Purview Records Management
- Module assessment
- Describe the data governance solutions of Microsoft Purview
 - Describe the concepts and benefits of data governance
 - Describe Microsoft Purview Data Map
 - Describe Microsoft Purview Unified Catalog
 - Module assessment

Objectives

Follow-on Courses

Browse the suggested follow-on courses below and continue your training journey. We offer training in various learning formats, from instructor-led to virtual, so you can choose what works best for you. Get started by selecting a course to learn more.

Security - Defend against cyberthreats with Microsoft's security operations platform

[View Details](#)

Security - Microsoft Identity and Access Administrator

[View Details](#)