Microsoft Security, Compliance, and Identity Fundamentals

Course SC-900T00: 1 day; Instructor-Led

Introduction

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

Audience

The audience for this course is looking to familiarize themselves with the fundamentals of 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.

Job role: Student
Preparation for exam: SC-900

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.

Course Outline

Module 1: Describe security and compliance concepts
Learn about common security and compliance concepts that are foundational to Microsoft solutions. Topics include the shared responsibility and Zero Trust models, encryption, data residency and data sovereignty, and more.

In this module, you will:

- Describe the shared responsibility and the defense-in-depth security models.
- Describe the Zero-Trust model.
- Describe the concepts of encryption and hashing.
- Describe some basic compliance concepts.

Lessons

- Introduction
- Describe the shared responsibility model
- Describe defense in depth
- Describe the Zero Trust model
- Describe encryption and hashing
- Describe compliance concepts

Module 2: Describe identity concepts
Learn about the key concepts of authentication and authorization and why identity is important in securing corporate resources. You'll also learn about some identity-related services.

In this module, you will:

- Understand the difference between authentication and authorization.
- Describe the concept of identity as a security perimeter.
- Describe identity-related services.

Lessons

- Introduction
- 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 3: Describe the services and identity types of Azure AD

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service. Learn about Azure AD, its services and the types of identities it supports.

In this module, you will:

- Describe what Azure AD does.
- Describe the types of identities Azure AD supports.

Lessons

- Introduction
- Describe Azure Active Directory
- Describe the available Azure AD editions
- Describe Azure AD identity types
- Describe the types of external identities
- Describe the concept of hybrid identity

Module 4: Describe the authentication capabilities of Azure AD

Learn about the authentication capabilities of Azure AD, multi-factor authentication, and how it improves security. You'll also learn about the password protection and management capabilities of Azure AD.

In this module, you will:

- Describe the authentication methods of Azure AD.
- Describe multi-factor authentication in Azure AD
- Describe the password protection and management capabilities of Azure AD.

Lessons

- Introduction
- Describe the authentication methods available in Azure AD
- Describe multi-factor authentication (MFA) in Azure AD
- Describe self-service password reset (SSPR) in Azure AD
- Describe password protection and management capabilities of Azure AD

Module 5: Describe the access management capabilities of Azure AD

A key function of Azure AD is to manage access. Learn about the access management capabilities, its use cases, and benefits.

In this module, you will:

- Describe Conditional Access in Azure AD.
- Describe the benefits of Azure AD roles and role-based access control.

Lessons

- Introduction
- Describe Conditional Access in Azure AD
- Describe the benefits of Azure AD roles and role-based access control

Module 6: Describe the identity protection and governance capabilities of Azure AD

Azure AD provides identity protection and governance capabilities. Learn about these capabilities, the use cases, and benefits.

In this module, you will:

- Describe the capabilities of identity governance in Azure.
- Describe Privileged Identity Management.
- Describe the capabilities of Azure Identity Protection.

Lessons

- Introduction
- Describe identity governance in Azure AD
- Describe what is entitlement management and access reviews
- Describe the capabilities of Privileged identity Management
- Describe Azure Identity Protection

Module 7: Describe basic security capabilities in Azure

Learn about capabilities Azure supports to protect your network, VMs, and your data.

In this module, you will:

- Learn how Azure security capabilities can protect the network
- Learn how Azure can protect your VMs
- Learn how encryption on Azure can protect your data

Lessons

- Introduction
- Describe Azure DDoS protection
- Describe Azure Firewall
- Describe Web Application Firewall
- Describe network segmentation in Azure
- Describe Azure Network Security groups
- Describe Azure Bastion and JIT Access
- Describe ways Azure encrypts data

Module 8: Describe security management capabilities of Azure

Learn about cloud security posture management and how Microsoft Defender for Cloud protects your cloud through secure score, recommendations, and enhanced features that provide cloud workload protection. You'll also learn about security baselines in Azure.

In this module, you will:

- Describe cloud security posture management.
- Describe the capabilities of Microsoft Defender for Cloud
- Understand the Microsoft cloud security benchmark and the security baselines in Azure.

Lessons

- Introduction
- Describe Cloud security posture management
- Describe Microsoft Defender for Cloud
- Describe the enhanced security of Microsoft Defender for Cloud
- Describe the Microsoft cloud security benchmark and security baselines for Azure

Module 9: Describe security capabilities of Microsoft Sentinel

Learn about Microsoft Sentinel a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution.

In this module, you will:

- Describe the security concepts for SIEM and SOAR.
- Describe how Microsoft Sentinel provides integrated threat management.
- Describe the pricing models of Microsoft Sentinel.

Lessons

- Introduction
- Define the concepts of SIEM and SOAR
- Describe how Microsoft Sentinel provides integrated threat management
- Understand Sentinel costs

Module 10: Describe threat protection with Microsoft 365 Defender

Protect against cyber threats with Microsoft 365 Defender across endpoints, identities, email, and applications.

In this module, you will:

- Describe the Microsoft 365 Defender service.
- Describe how Microsoft 365 Defender provides integrated protection against sophisticated attacks.
- Describe and explore Microsoft 365 Defender portal.

Lessons

- Introduction
- Describe Microsoft 365 Defender services
- Describe Microsoft Defender for Office 365
- Describe Microsoft Defender for Endpoint
- Describe Microsoft Defender for Cloud Apps
- Describe Microsoft Defender for Identity
- Describe the Microsoft 365 Defender portal

Module 11: Describe the Service Trust Portal and privacy at Microsoft

Microsoft runs on trust! Here you'll explore the Service Trust Portal for content on how Microsoft delivers on our commitment of trust. You'll also learn about Microsoft Priva, a solution to help meet privacy goals.

In this module, you will:

- Describe the offerings of the Service Trust Portal.
- Describe Microsoft's Privacy principles.
- Describe Microsoft Priva.

Lessons

- Introduction
- Describe the Service Trust Portal
- Describe Microsoft's privacy principles
- Describe Microsoft Priva

Module 12: Describe the compliance management capabilities in Microsoft Purview

Explore the Microsoft Purview compliance portal, the portal for organizations to manage their compliance needs. Learn about the Compliance Manager and compliance score, which can help organizations manage, simplify, and improve compliance across their organization.

In this module, you will:

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

Lessons

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

Module 13: Describe information protection and data lifecycle management in Microsoft Purview
Information protection and data lifecycle management in Microsoft Purview helps organizations classify, protect, and retain their data where it lives and wherever it goes. Learn about data classification capabilities, data loss prevention, and records management.

In this module, you will:
- Describe data classification capabilities
- Describe records management
- Describe data loss prevention

Lessons
- Introduction
- Know your data, protect your data, and govern your data
- Describe the data classification capabilities of the compliance portal
- Describe sensitivity labels and policies
- Describe data loss prevention
- Describe retention policies and retention labels
- Describe records management

Module 14: Describe insider risk capabilities in Microsoft Purview
Insider risks are a top concern for organizations. These risks can be challenging to identify and mitigate. Learn how Microsoft Purview enables organizations to identify, analyze, and remediate internal risks before they cause harm.

In this module, you will:
- Describe insider risk management
- Describe communication compliance
- Describe information barriers

Lessons
- Introduction
- Describe insider risk management
- Describe communication compliance
- Describe information barriers

Module 15: Describe the eDiscovery and audit capabilities of Microsoft Purview
Organizations may need to identify, collect, and/or audit information for legal, regulatory, or business reasons. Learn how the eDiscovery and audit capabilities of Microsoft Purview help organizations find relevant data quickly.

In this module, you will:
- Describe the eDiscovery capabilities of Microsoft Purview.
- Describe the auditing capabilities of Microsoft Purview.

Lessons
- Introduction
- Describe the eDiscovery solutions in Microsoft Purview
- Describe the audit solutions in Microsoft Purview

Module 16: Describe resource governance capabilities in Azure
Azure governance capabilities provide mechanisms and processes for organizations to maintain control over their applications and resources. Learn how Azure policy, Blueprints, and Microsoft Purview help organizations govern their resources and applications.

In this module, you will:
- Describe Azure Policy.
- Describe Azure Blueprints
- Describe Microsoft Purview

Lessons

- Introduction
- Describe Azure Policy
- Describe the use of Azure Blueprints
- Describe the capabilities in the Microsoft Purview governance portal

