

## MS-SC900T00: INTRODUCTION TO MICROSOFT SECURITY, COMPLIANCE, AND IDENTITY



DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
1 Day	Beginner	Security	Instructor-led	NA

### INTRODUCTION

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

### AUDIENCE PROFILE

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.

### 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 OBJECTIVES

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.

### COURSE CONTENT

#### 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.

##### Lessons

- Introduction
- 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

After completing this module, students will be able to:

- Describe the shared responsibility and the defence-in-depth security models.
- Describe the Zero-Trust model.

- Describe the concepts of encryption and hashing.
- Describe some basic 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.

##### Lessons

- 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.
- Knowledge check.

After completing this module, students will be able to:

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

#### Module 3: Describe the function and identity types of Microsoft Entra ID

Microsoft Entra ID is Microsoft's cloud-based identity and access management solution that connects people to their apps, devices, and data. Learn about the functions and identity types supported by Microsoft Entra ID.

##### Lessons

- Describe Microsoft Entra ID.
- Describe types of identities.
- Describe hybrid identity.
- Describe external identities.
- Knowledge check.

After completing this module, students will be able to:

- Describe the function of Microsoft Entra ID.

- Describe the types of identities Microsoft Entra ID supports.

## Module 4: Describe the authentication capabilities of Microsoft Entra ID

Learn about the authentication capabilities of Microsoft Entra ID, including multifactor authentication, and how they improve security. You'll also learn about self-service password reset (SSPR) and the password protection and management capabilities.

### Lessons

- Describe authentication methods.
- Describe multifactor authentication.
- Describe self-service password reset.
- Describe password protection and management capabilities.
- Knowledge check.

After completing this module, students will be able to:

- Describe the authentication methods of Microsoft Entra ID.
- Describe multifactor authentication (MFA) in Microsoft Entra ID.
- Describe self-service password reset (SSPR) in Microsoft Entra ID.
- Describe the password protection and management capabilities of Microsoft Entra ID.

## Module 5: Describe access management capabilities of Microsoft Entra ID

A key function of Microsoft Entra ID is to manage access. Learn about the conditional access and how Microsoft Entra roles and role-based access control (RBAC) helps organizations manage and control access.

### Lessons

- Introduction.
- Describe Conditional Access.
- Describe Microsoft Entra roles and role-based access control (RBAC).
- Knowledge check.

After completing this module, students will be able to:

- Describe Conditional Access in Microsoft Entra ID.
- Describe Microsoft Entra roles and role-based access control.
- Describe Global Secure Access in Microsoft Entra.

## Module 6: Describe the identity protection and governance capabilities of Microsoft Entra

Microsoft Entra provides identity protection and governance capabilities. Learn about these capabilities, the use cases, and benefits.

### Lessons

- 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 integration with Microsoft Security Copilot.
- Describe Microsoft Entra Verified ID.
- Knowledge check.

After completing this module, students will be able to:

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

## Module 7: Describe Microsoft Security Copilot

Get acquainted with Microsoft Security Copilot. You are introduced to some basic terminology, how Microsoft Security Copilot processes prompts, the elements of an effective prompt, and how to enable the solution.

### Lessons

- Introduction
- 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

By the end of this module, you'll be able to:

- Describe what Microsoft Security Copilot is.
- Describe the terminology of Microsoft Security Copilot.
- Describe how Microsoft Security Copilot processes prompt requests.
- Describe the elements of an effective prompt
- Describe how to enable Microsoft Security Copilot.

## Module 8: Describe core infrastructure security services in Azure

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

### Lessons

- 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.
- Knowledge check.

After completing this module, students will be able to:

- Learn how Azure security capabilities can protect the network
- Learn how Azure can protect your VMs
- Learn how to keep secrets safe with Azure Key Vault

## Module 9: Describe the security management capabilities in Azure

Learn about Microsoft Defender for Cloud and the capabilities it brings together to protect your cloud through secure score, recommendations, and enhanced features that provide cloud workload protection.

### Lessons

- Describe Microsoft Defender for Cloud.
- Describe how security policies and initiatives improve cloud security posture.
- Describe Cloud security posture management.
- Describe the enhanced security of Microsoft Defender for Cloud.
- Describe DevOps security management.
- Knowledge check.

After completing this module, students will be able to:

- Describe Microsoft Defender for Cloud.
- Describe how security policies and initiatives improve cloud security posture.
- Describe how the three pillars of Microsoft Defender for Cloud protect against cyber threats and vulnerabilities.

## Module 10: Describe the capabilities in 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'll also be introduced to Microsoft Security Copilot.

### Lessons

- Define the concepts of SIEM and SOAR.

- Describe threat detection and mitigation capabilities in Microsoft Sentinel.
- Describe Microsoft Security Copilot.
- Knowledge check.

After completing this module, students will be able to:

- Describe the security concepts for SIEM and SOAR.
- Describe how Microsoft Sentinel provides threat detection and mitigation.
- Describe Microsoft Security Copilot.

## Module 11: Describe threat protection with Microsoft Defender XDR

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

Lessons

- 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 the Microsoft 365 Defender portal.
- Knowledge check

After completing this module, students will be able to:

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

## Module 12: Describe Microsoft's Service Trust portal and privacy capabilities.

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 Privacy, a solution to help meet privacy goals.

Lessons

- Describe the offerings of the Service Trust portal.
- Describe Microsoft's privacy principles.
- Describe Microsoft Privacy.
- Knowledge check.

After completing this module, students will be able to:

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

## Module 13: Describe the data security solutions of Microsoft Purview

Describe the data security solutions of Microsoft Purview.

Lessons

- Introduction
- 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
- Module assessment
- Summary

After completing this module, students will be able to:

- Describe how Microsoft Purview Information Protection helps organizations discover, classify, and protect sensitive information.
- Describe how Microsoft Purview Data Loss Prevention helps organizations prevent their users from inappropriately sharing sensitive data with people who shouldn't have it.
- Describe how Microsoft Purview Insider Risk Management helps minimize internal risks.

## Module 14: Describe the data compliance solutions of Microsoft Purview

Learn how Microsoft Purview data compliance solutions help organizations manage risk and regulatory requirements.

Lessons

- Introduction
- Describe audit in Microsoft Purview
- Describe eDiscovery
- Describe Compliance Manager
- Describe Communication Compliance
- Describe Data Lifecycle Management
- Describe Records Management
- Module assessment
- Summary

After completing this module, students will be able to:

- Describe Microsoft Purview eDiscovery and Audit
- Describe Microsoft Purview Compliance Manager
- Describe Microsoft Purview Communication Compliance
- Describe Microsoft Purview Data Lifecycle Management
- Describe Microsoft Purview Records Management

## Module 15: Describe the data governance solutions of Microsoft Purview

Learn about Microsoft Purview data governance solutions that leverage AI and modern technologies to ensure data quality, security, and compliance while also accelerating value creation.

Lessons

- Introduction
- Describe the concepts and benefits of data governance
- Describe Microsoft Purview Data Catalog
- Module assessment
- Summary

After completing this module, students will be able to:

- Describe the concepts and benefits of data governance.
- Describe the capabilities of Microsoft Purview Data Catalog.

## ASSOCIATED CERTIFICATION & EXAM

This course will prepare delegates to write the Microsoft SC900: Microsoft Security, Compliance, and Identity Fundamentals exam.