Microsoft Security, Compliance, and Identity Fundamentals SC-900T00-A

Course Duration: 8 Hours (1 Day)

Overview

The Microsoft Security, Compliance, and Identity Fundamentals SC-900T00-A course is designed to provide learners with foundational knowledge of security, compliance, and Identity management across cloud-based and related Microsoft services. The course is divided into four modules, each focusing on a different aspect of Microsoft's security and compliance capabilities. In Module 1, participants are introduced to the basic concepts of security, compliance, and identity, setting the stage for a deeper dive into these areas. Module 2 covers the capabilities of Microsoft Azure Active Directory (Azure AD), which is an integral part of Microsoft Entra. This module provides hands-on labs to explore Azure AD services, Authentication, Access management, and Identity protection. Module 3 focuses on the security solutions available within Microsoft's ecosystem, including Azure security features, Azure Sentinel, and Microsoft 365 Defender. Learners will engage with labs to gain practical experience with these tools. Lastly, Module 4 delves into Microsoft's compliance solutions, discussing the Information protection, Governance, eDiscovery, and Audit capabilities provided by Microsoft Purview and other tools, complemented by practical labs. This course will benefit learners by equipping them with the skills to understand and leverage Microsoft's security and compliance features to protect data and comply with legal and regulatory standards.

Audience Profile

The Microsoft SC-900 course offers foundational knowledge in security, compliance, and identity across cloud-based and related Microsoft services.

- IT professionals looking to understand Microsoft security and compliance solutions
- Security administrators seeking knowledge of Microsoft's security, compliance, and identity ecosystem
- Compliance officers who need to grasp Microsoft's compliance solutions
- Systems administrators aiming to learn about Azure Active Directory and Microsoft security capabilities
- Network administrators interested in Azure's security management and threat protection
- Identity managers exploring identity concepts and Azure AD's identity protection and governance
- Data protection officers requiring insight into Microsoft 365's information protection and governance
- IT support staff who provide troubleshooting and support for security-related issues
- Risk management professionals wanting to understand Microsoft's insider risk capabilities
- Legal professionals or paralegals involved in eDiscovery and audit processes within Microsoft solutions
- Cloud architects interested in Microsoft's security and compliance features

- Security-focused sales engineers and pre-sales architects who advise clients on Microsoft 365 and Azure security solutions
- Fresh graduates and IT enthusiasts beginning their career in cloud security and compliance
- Business stakeholders who need to ensure their organization meets compliance standards with Microsoft tools
- Managed service providers offering security and compliance services for Microsoft environments
- Cybersecurity consultants looking to expand their knowledge of Microsoft security solutions
- Government officials or employees in regulatory roles who oversee or implement compliance standards
- Security trainers and educators who provide training on Microsoft security and compliance solutions
- Technical decision-makers evaluating or planning to implement Microsoft security and compliance solutions in their organizations
- Professionals preparing for the Microsoft Security, Compliance, and Identity Fundamentals certification exam

Course Syllabus

Module 1: Describe the concepts of security, compliance, and identity

Learn about core concepts that are foundational to security, compliance, and identity solutions, including shared responsibility, Zero Trust, data residency, the role of identity providers, and more.

Lessons:

- Describe security and compliance concepts
- Describe identity concepts

After completing this module, students will be able to:

- Describe security and compliance concepts.
- Describe identity concepts.

Module 2: Describe the capabilities of Microsoft Azure Active Directory, part of Microsoft Entra

Azure Active Directory is the tool for identity and access management in the Microsoft Cloud. Learn about Azure AD services and identity principals, secure authentication, access management capabilities, as well as identity protection and governance.

Lessons:

- Describe the basic services and identity types of Azure AD
- Describe the authentication capabilities of Azure AD

- Describe the access management capabilities of Azure AD
- Describe the identity protection and governance capabilities of Azure AD

Lab: Explore Azure Active Directory

Lab: Explore Azure AD Authentication with self-service password reset

Lab: Explore access management in Azure AD with Conditional Access

Lab: Explore identity governance in Azure AD with Privileged Identity Management

After completing this module, students will be able to:

- Describe the basic services and identity types of Azure AD.
- Describe the authentication capabilities of Azure AD.
- Describe the access management capabilities of Azure AD.
- Describe the identity protection and governance capabilities of Azure AD

Module 3: Describe the capabilities of Microsoft security solutions

Learn about Microsoft's security solutions. Topics covered include network and platform capabilities of Azure, Azure security management with Microsoft Defender for Cloud, and Microsoft Sentinel. You'll learn about threat protection with Microsoft 365 Defender.

Lessons:

- Describe the basic security capabilities in Azure
- Describe the security management capabilities of Azure
- Describe the security capabilities of Microsoft Sentinel
- Describe the threat protection capabilities of Microsoft 365 Defender

Lab: Explore Microsoft Defender for Cloud Apps

Lab: Explore Microsoft Sentinel

Lab: Explore Microsoft Defender for Cloud

Lab: Explore Azure Network Security Groups (NSGs)

Lab: Explore the Microsoft 365 Defender portal

After completing this module, students will be able to:

- Describe the basic security capabilities in Azure.
- Describe the security management capabilities of Azure.
- Describe the security capabilities of Microsoft Sentinel.
- Describe the threat protection capabilities of Microsoft 365 Defender.

Module 4: Describe the capabilities of Microsoft compliance solutions

Learn about Microsoft's Service Trust Portal and privacy at Microsoft. You'll learn about Microsoft Purview, a comprehensive set of solutions that help you govern, protect, and manage your entire data estate. You'll also learn about Azure resource governance capabilities.

Lessons:

- Describe the Service Trust Portal and privacy at Microsoft
- Describe the compliance management capabilities of Microsoft Purview
- Describe information protection and data lifecycle management in Microsoft Purview
- Describe the insider risk capabilities in Microsoft Purview
- Describe the eDiscovery and audit capabilities of Microsoft Purview
- Describe the resource governance capabilities in Azure

Lab: Explore the Core eDiscovery workflow

Lab: Explore Azure Policy

Lab: Explore the Service Trust Portal

Lab: Explore the Microsoft Purview compliance portal & Compliance Manager

Lab: Explore sensitivity labels in Microsoft Purview

Lab: Explore insider risk management in Microsoft Purview

After completing this module, students will be able to:

- Describe the Service Trust Portal and privacy at Microsoft.
- Describe the compliance management capabilities of Microsoft Purview.
- Describe information protection and data lifecycle management in Microsoft Purview.
- Describe the insider risk capabilities in Microsoft Purview.
- Describe the eDiscovery and audit capabilities of Microsoft Purview.
- Describe the resource governance capabilities in Azure