PURPLE GRIFFON
The IT Service Management Training & Consultancy Specialists

Course Title: SC-900T00 Microsoft Security, Compliance, and Identity	**Course Duration**: 1.0 Day
Exam: Not Included	**Exam Type**: Proctored Exam
Qualification: SC-900 Completion Certificate	

Course Syllabus

1 - Describe security and compliance concepts

- Describe the shared responsibility model
- Describe defense in depth
- Describe the Zero Trust model
- Describe governance, risk, and compliance (GRC) concepts

2 - 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

3 - Describe the function and identity types of Microsoft Entra ID

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

4 - 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

5 - Describe access management capabilities of Microsoft Entra ID

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

6 - Describe the identity protection and governance capabilities of Azure AD

- 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 Permissions Management
- Describe Microsoft Entra Verified ID

7 - 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

8 - Describe the security management capabilities in Azure

- 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

9 - Describe security capabilities of Microsoft Sentinel

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

10 - 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 the Microsoft Defender portal

11 - Describe Microsofts Service Trust portal and privacy capabilities

- Describe the offerings of the Service Trust portal
- Describe Microsoft's privacy principles
- Describe Microsoft Priva

12 - Describe the compliance management capabilities in Microsoft Purview

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

13 - Describe information protection, data lifecycle management, and data governance capabilities in Microsoft Purview

- 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
- Describe the Microsoft Purview unified data governance solution

14 - Describe the insider risk capabilities in Microsoft Purview

- Describe insider risk management
- Describe communication compliance

15 - Describe the eDiscovery and Audit capabilities in Microsoft Purview

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

Course Overview

This course provides a foundational understanding of security, compliance, and identity (SCI) concepts in Microsoft environments. It covers core principles of security, identity management, compliance, and governance using Microsoft solutions such as Microsoft Entra ID, Microsoft 365 Security and Compliance tools, and Azure security services. Learners gain practical knowledge to help protect organizational data, manage user access, and meet regulatory requirements.

Course Learning Outcomes

By the end of this course, learners will be able to describe the principles of security, compliance, and identity, explain core Microsoft identity and access management concepts, understand security solutions in Microsoft 365 and Azure, identify compliance features and regulatory requirements, and apply foundational knowledge of governance, risk, and compliance tools. This provides a strong base for entry-level security and compliance roles or further Microsoft certifications.

Audience

Beginners in IT, business users, IT administrators, security professionals, and anyone seeking foundational knowledge of Microsoft security, compliance, and identity

Entry-Level Requirements

No prior Microsoft experience required; general IT or business knowledge recommended

Recommended Reading

Microsoft Learn SC-900 learning path, Microsoft Trust Center documentation, Microsoft Entra ID and Security & Compliance guides

What's Included

Instructor-led training, course materials, exam preparation guide

Exam Information

This course prepares learners for the SC-900: Microsoft Security, Compliance, and Identity Fundamentals certification exam. The exam measures foundational knowledge of security, compliance, and identity concepts, as well as Microsoft security solutions and governance features. The exam includes multiple-choice and scenario-based questions. Passing the exam earns the official Microsoft Certified: Security, Compliance, and Identity Fundamentals credential.

What's Next

After completing SC-900, learners can progress to role-based certifications such as SC-200 (Security Operations Analyst), SC-300 (Identity and Access Administrator), or SC-400 (Information Protection Administrator) to specialize in Microsoft security and compliance.

Additional Information

Prerequisites

- 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.