Microsoft Security, Compliance, and Identity Fundamentals: SC-900

EXAM DESIGN

Audience Profile

This certification is targeted to those looking to familiarize themselves with the fundamentals of security, compliance, and identity (SCI) across cloud-based and related Microsoft services.

This is a broad audience that may include business stakeholders, new or existing IT professionals, or students who have an interest in Microsoft security, compliance, and identity solutions.

Candidates should be familiar with Microsoft Azure and Microsoft 365 and want to understand how Microsoft security, compliance, and identity solutions can span across these solution areas to provide a holistic and end-to-end solution.

Objective Domains

SKILLS MEASURED

- NOTE: The bullets that follow each of the skills measured are intended to illustrate how we are assessing that skill. Related topics may be covered in the exam.
- NOTE: Most questions cover features that are general availability (GA). The exam may contain questions on Preview features if those features are commonly used.

Describe the concepts of security, compliance, and identity (10-15%)

Describe security and compliance concepts

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

Define identity concepts

- Define identity as the primary security perimeter
- Define authentication
- Define authorization
- Describe identity providers
- Describe Active Directory
- Describe the concept of Federation

Microsoft Security, Compliance, and Identity Fundamentals

Describe the capabilities of Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra (25-30%)

Describe the basic identity services and identity types of Azure AD

- Describe Azure Active Directory
- Describe Azure AD identities
- Describe hybrid identity
- Describe the different external identity types

Describe the authentication capabilities of Azure AD

- Describe the authentication methods available in Azure AD
- Describe Multi-factor Authentication
- Describe self-service password reset
- Describe password protection and management capabilities available in Azure AD

Describe access management capabilities of Azure AD

- Describe conditional access
- Describe the benefits of Azure AD roles.
- Describe the benefits of Aure AD role-based access control

Describe the identity protection and governance capabilities of Azure AD

- Describe identity governance in Azure AD
- Describe entitlement management and access reviews
- Describe the capabilities of Azure AD Privileged Identity Management (PIM)
- Describe Azure AD Identity Protection

Describe the capabilities of Microsoft Security solutions (25—30%)

Describe basic security capabilities in Azure

- Describe Azure DDoS protection
- Describe Azure Firewall
- Describe Web Application Firewall
- Describe Network Segmentation with VNet
- Describe Azure Network Security groups
- Describe Azure Bastion and JIT Access
- Describe ways Azure encrypts data

Describe security management capabilities of Azure

- Describe Cloud security posture management (CSPM)
- Describe Microsoft Defender for Cloud
- Describe the enhanced security features of Microsoft Defender for Cloud
- Describe security baselines for Azure

Describe security capabilities of Microsoft Sentinel

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

Describe threat protection with Microsoft 365 Defender

- Describe Microsoft 365 Defender services
- Describe Microsoft Defender for Identity (formerly Azure ATP)
- Describe Microsoft Defender for Office 365 (formerly Office 365 ATP)
- Describe Microsoft Defender for Endpoint (formerly Microsoft Defender ATP)
- Describe Microsoft Defender for Cloud Apps
- Describe the Microsoft 365 Defender portal

Describe the capabilities of Microsoft compliance solutions (25—30%)

Describe Microsoft's Service Trust Portal and privacy principles

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

Describe the compliance management capabilities of Microsoft Purview

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

Describe information protection and data lifecycle management capabilities of Microsoft Purview

- Describe data classification capabilities
- Describe the benefits of content and activity explorer
- Describe sensitivity labels
- Describe Data Loss Prevention (DLP)
- Describe Records Management
- Describe Retention Polices, Retention Labels and retention label policies

Describe insider risk capabilities in Microsoft Purview

- Describe Insider Risk Management
- Describe communication compliance
- Describe information barriers

Describe resource governance capabilities in Azure

- Describe Azure Policy
- Describe Azure Blueprints
- Describe the capabilities in the Microsoft Purview