Exam SC-900: Microsoft Security, Compliance, and Identity Fundamentals – Skills Measured

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.

Skills Measured

NOTE: The bullets that appear below each of the skills measured are intended to illustrate how we are assessing that skill. This list is not definitive or exhaustive.

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 (5-10%)

Describe security methodologies

- describe the Zero-Trust methodology
- describe the shared responsibility model
- define defense in depth

Describe security concepts

- describe common threats
- describe encryption

Describe Microsoft Security and compliance principles

- describe Microsoft's privacy principles

- describe the offerings of the service trust portal

Describe the capabilities of Microsoft Identity and Access Management Solutions (25-30%)

Define identity principles/concepts

- define identity as the primary security perimeter
- define authentication
- define authorization
- describe what identity providers are
- describe what Active Directory is
- describe the concept of Federated services
- define common Identity Attacks

Describe the basic identity services and identity types of Azure AD

- describe what Azure Active Directory is
- describe Azure AD identities (users, devices, groups, service principals/applications)
- describe what hybrid identity is
- describe the different external identity types (Guest Users)

Describe the authentication capabilities of Azure AD

- describe the different authentication methods
- describe self-service password reset
- describe password protection and management capabilities
- describe Multi-factor Authentication
- describe Windows Hello for Business

Describe access management capabilities of Azure AD

- describe what conditional access is
- describe uses and benefits of conditional access
- describe the benefits of Azure AD roles

Describe the identity protection & governance capabilities of Azure AD

- describe what identity governance is
- describe what entitlement management and access reviews is
- describe the capabilities of PIM
- describe Azure AD Identity Protection

Describe the capabilities of Microsoft Security Solutions (30-35%)

Describe basic security capabilities in Azure

- describe Azure Network Security groups
- describe Azure DDoS protection
- describe what Azure Firewall is
- describe what Azure Bastion is
- describe what Web Application Firewall is
- describe ways Azure encrypts data

Describe security management capabilities of Azure

- describe the Azure Security center
- describe Azure Secure score
- describe the benefit and use cases of Azure Defender - previously the cloud workload protection platform (CWPP)
- describe Cloud security posture management (CSPM)
- describe security baselines for Azure

Describe security capabilities of Azure Sentinel

- define the concepts of SIEM, SOAR, XDR
- describe the role and value of Azure Sentinel to provide integrated threat protection

Describe threat protection with Microsoft 365 Defender (formerly Microsoft Threat Protection)

- 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 Cloud App Security

Describe security management capabilities of Microsoft 365

- describe the Microsoft 365 Security Center
- describe how to use Microsoft Secure Score
- describe security reports and dashboards
- describe incidents and incident management capabilities

Describe endpoint security with Microsoft Intune

- describe what Intune is

- describe endpoint security with Intune
- describe the endpoint security with the Microsoft Endpoint Manager admin center

Describe the Capabilities of Microsoft Compliance Solutions (25-30%)

Describe the compliance management capabilities in Microsoft

- describe the compliance center
- describe compliance manager
- describe use and benefits of compliance score

Describe information protection and governance capabilities of Microsoft 365

- describe data classification capabilities
- describe the value of content and activity explorer
- describe sensitivity labels
- describe Retention Polices and Retention Labels
- describe Records Management
- describe Data Loss Prevention

Describe insider risk capabilities in Microsoft 365

- describe Insider risk management solution
- describe communication compliance
- describe information barriers
- describe privileged access management
- describe customer lockbox

Describe the eDiscovery capabilities of Microsoft 365

- describe the purpose of eDiscovery
- describe the capabilities of the content search tool
- describe the core eDiscovery workflow
- describe the advanced eDisovery workflow

Describe the audit capabilities in Microsoft 365

- describe the core audit capabilities of M365
- describe purpose and value of Advanced Auditing

Describe resource governance capabilities in Azure

- describe the use of Azure Resource locks
- describe what Azure Blueprints is

- define Azure Policy and describe its use cases
- describe cloud adoption framework