Microsoft Certified: Security, Compliance, and Identity Fundamentals – Skills Measured

This document contains the skills measured on the exams associated with this certification. It does not include any upcoming or recent changes that have been made to those skills. For more information about upcoming or recent changes, see the associated exam details page(s).

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.

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

Describe the Concepts of Security, Compliance, and Identity (5-10%)

Describe security and compliance concepts & methodologies

- describe the Zero-Trust methodology
- describe the shared responsibility model
- define defense in depth
- describe common threats
- describe encryption and hashing
- describe cloud adoption framework

Define identity 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 capabilities of Microsoft Identity and Access Management Solutions (25-30%)

Describe the basic identity services and identity types of Azure AD

- describe what Azure Active Directory is
- describe Azure AD identity types (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 Cloud security posture management (CSPM)
- describe Microsoft Defender for Cloud
- describe secure score in Microsoft Defender Cloud

- describe enhanced security of Microsoft Defender for Cloud
- describe security baselines for Azure

Describe security capabilities of Microsoft Sentinel

- define the concepts of SIEM, SOAR, XDR
- describe how of Microsoft Sentinel provides integrated threat protection

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 security management capabilities of Microsoft 365

- describe the Microsoft 365 Defender portal
- 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 offerings of the Service Trust portal
- describe Microsoft's privacy principles
- 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 and audit 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 eDiscovery workflow
- 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