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

---

The English language version of this exam will be updated on April 25, 2022.

Following the current exam guide, we have included a table that compares the current study guide to the new one by functional group, showing the changes that will be made to the exam on that date.

NOTE: Passing score: 700. Learn more about exam scores.

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 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 (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
- 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

The table below shows the changes that will be implemented on April 25, 2022 to the English language version of this exam. Following the comparison table, the revised exam guide is included.

Old objective number	**Subtask changes and new location**
1.1 Describe security and compliance concepts & methodologies	Revised title and subtasks
1.2 Define identity concepts	Revised subtasks
2.1 Describe the basic identity services and identity types of Azure AD	Revised subtasks
2.2 Describe the authentication capabilities of Azure AD	Revised subtasks
2.3 Describe access management capabilities of Azure AD	Revised subtasks
2.4 Describe the identity protection & governance capabilities of Azure AD	Revised subtasks
3.1 Describe basic security capabilities in Azure	Revised subtasks
3.2 Describe security management capabilities of Azure	Revised subtasks
3.3 Describe security capabilities of Azure Sentinel	Revised subtasks
3.4 Describe threat protection with Microsoft 365 Defender	Revised subtasks
3.5 Describe security management capabilities of Microsoft 365	Deleted; moved to 3.4
3.6 Describe endpoint security with Microsoft Intune	Deleted
4.1 Describe the compliance management capabilities in Microsoft	Revised title and subtasks, split into 4.1 and 4.2
4.2 Describe information protection and governance capabilities of Microsoft 365	Revised title and subtasks
4.3 Describe insider risk capabilities in Microsoft 365	Revised subtasks
4.4 Describe resource governance capabilities in Azure	Revised title and subtasks

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 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 are
- describe Azure Active Directory
- describe the concept of Federation

Describe the capabilities of Microsoft identity and access management solutions (25-30%)

Describe the basic identity services and identity types of Azure AD

- describe Azure Active Directory (AD)
- describe Azure AD identities
- describe what 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 what conditional access is.
- describe the benefits of Azure AD roles
- describe the benefits of Azure AD role-based access control

Describe the identity protection & governance capabilities of Azure AD

- describe identity governance in Azure AD
- describe entitlement management and access reviews
- describe the capabilities of 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 Azure VNet
- describe Azure Network Security groups
- describe Azure Bastion and JIT Access
- describe the ways Azure encrypts data

Describe security management capabilities of Azure

- describe Cloud security posture management (CSPM)
- describe Microsoft Defender for Cloud
- describe 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 Office 365
- describe Microsoft Defender for Endpoint

- describe Microsoft Defender for Cloud Apps
- describe Microsoft Defender for Identity
- describe the Microsoft 365 Defender portal

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

Describe the compliance management capabilities of Microsoft

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

Describe the compliance management capabilities of Microsoft 365

- describe Microsoft 365 compliance center
- describe compliance manager
- describe the use of benefits of compliance score

Describe information protection and governance capabilities of Microsoft 365

- 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 and Retention Labels

Describe insider risk capabilities in Microsoft 365

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

Describe resource governance capabilities in Azure

- describe what Azure Blueprints is
- describe Azure Policy
- describe Azure Blueprint
- describe Azure Purview