

# Study guide for Exam SC-900: Microsoft Security, Compliance, and Identity Fundamentals

## Purpose of this document

This study guide should help you understand what to expect on the exam and includes a summary of the topics the exam might cover and links to additional resources. The information and materials in this document should help you focus your studies as you prepare for the exam.

Useful links	Description
<a href="#">Review the skills measured as of May 5, 2023</a>	This list represents the skills measured AFTER the date provided. Study this list if you plan to take the exam AFTER that date.
<a href="#">Review the skills measured prior to May 5, 2023</a>	Study this list of skills if you take your exam PRIOR to the date provided.
<a href="#">Change log</a>	You can go directly to the change log if you want to see the changes that will be made on the date provided.
<a href="#">How to earn the certification</a>	Some certifications only require passing one exam, while others require passing multiple exams.
<a href="#">Your Microsoft Learn profile</a>	Connecting your certification profile to Microsoft Learn allows you to schedule and renew exams and share and print certificates.
<a href="#">Exam scoring and score reports</a>	A score of 700 or greater is required to pass.
<a href="#">Exam sandbox</a>	You can explore the exam environment by visiting our exam sandbox.
<a href="#">Request accommodations</a>	If you use assistive devices, require extra time, or need modification to any part of the exam experience, you can request an accommodation.

Useful links	Description
<a href="#">Take a free Practice Assessment</a>	Test your skills with practice questions to help you prepare for the exam.

## Updates to the exam

Our exams are updated periodically to reflect skills that are required to perform a role. We have included two versions of the Skills Measured objectives depending on when you are taking the exam.

We always update the English language version of the exam first. Some exams are localized into other languages, and those are updated approximately eight weeks after the English version is updated. While Microsoft makes every effort to update localized versions as noted, there may be times when the localized versions of an exam are not updated on this schedule. Other available languages are listed in the **Schedule Exam** section of the **Exam Details** webpage. If the exam isn't available in your preferred language, you can request an additional 30 minutes to complete the exam.

### 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.

## Skills measured as of May 5, 2023

### 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.

- Describe the concepts of security, compliance, and identity (10–15%)
- Describe the capabilities of Microsoft Azure Active Directory, part of Microsoft Entra (25–30%)
- Describe the capabilities of Microsoft Security solutions (25–30%)
- Describe the capabilities of Microsoft compliance solutions (25–30%)

## **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

## **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 AD
- 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 Azure 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 Azure Virtual Networks
- 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 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 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 explorer and activity explorer
- Describe sensitivity labels and sensitivity label policies
- Describe Data Loss Prevention (DLP)
- Describe Records Management
- Describe Retention Policies, 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 Microsoft Purview unified data governance solution

## Study resources

We recommend that you train and get hands-on experience before you take the exam. We offer self-study options and classroom training as well as links to documentation, community sites, and videos.

Study resources	Links to learning and documentation
<b>Get trained</b>	<a href="#">Choose from self-paced learning paths and modules or take an instructor-led course</a>
<b>Find documentation</b>	<a href="#">Microsoft security documentation</a> <a href="#">Azure security documentation</a> <a href="#">Azure Active Directory documentation</a> <a href="#">Microsoft Sentinel documentation</a> <a href="#">Microsoft 365 Defender documentation</a> <a href="#">Microsoft Purview</a> <a href="#">Get started with the Microsoft Service Trust Portal</a>
<b>Ask a question</b>	<a href="#">Microsoft Q&amp;A   Microsoft Docs</a>

Study resources	Links to learning and documentation
Get community support	<a href="#">Security, compliance, and identity community hub</a>
Follow Microsoft Learn	<a href="#">Microsoft Learn - Microsoft Tech Community</a>
Find a video	<a href="#">Exam Readiness Zone</a> <a href="#">Microsoft Learn Shows</a>

## Change log

Key to understanding the table: The topic groups (also known as functional groups) are in bold typeface followed by the objectives within each group. The table is a comparison between the two versions of the exam skills measured and the third column describes the extent of the changes.

Skill area prior to May 5, 2023	Skill area prior to May 5, 2023	Change
Audience profile		No change
<b>Describe the concepts of security, compliance, and identity</b>	<b>Describe the concepts of security, compliance, and identity</b>	No change
Describe security and compliance concepts	Describe security and compliance concepts	No change
Define identity concepts	Define identity concepts	No change
<b>Describe the capabilities of Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra</b>	<b>Describe the capabilities of Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra</b>	No change
Describe the basic identity services and identity types of Azure AD	Describe the basic identity services and identity types of Azure AD	No change
Describe the authentication capabilities of Azure AD	Describe the authentication capabilities of Azure AD	No change
Describe access management capabilities of Azure AD	Describe access management capabilities of Azure AD	No change
Describe the identity protection and governance capabilities of Azure AD	Describe the identity protection and governance capabilities of Azure AD	No change
<b>Describe the capabilities of Microsoft Security solutions</b>	<b>Describe the capabilities of Microsoft Security solutions</b>	No change

Skill area prior to May 5, 2023	Skill area prior to May 5, 2023	Change
Describe basic security capabilities in Azure	Describe basic security capabilities in Azure	No change
Describe security management capabilities of Azure	Describe security management capabilities of Azure	No change
Describe security capabilities of Microsoft Sentinel	Describe security capabilities of Microsoft Sentinel	No change
Describe threat protection with Microsoft 365 Defender	Describe threat protection with Microsoft 365 Defender	No change
<b>Describe the capabilities of Microsoft compliance solutions</b>	<b>Describe the capabilities of Microsoft compliance solutions</b>	No change
Describe Microsoft's Service Trust Portal and privacy principles	Describe Microsoft's Service Trust Portal and privacy principles	No change
Describe the compliance management capabilities of Microsoft Purview	Describe the compliance management capabilities of Microsoft Purview	No change
Describe information protection and data lifecycle management capabilities of Microsoft Purview	Describe information protection and data lifecycle management capabilities of Microsoft Purview	Minor
Describe insider risk capabilities in Microsoft Purview	Describe insider risk capabilities in Microsoft Purview	No change
Describe resource governance capabilities in Azure	Describe resource governance capabilities in Azure	No change

## Skills measured prior to May 5, 2023

### 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.

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

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

## **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

## **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 AD
- 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 Azure 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 Azure Virtual Networks
- 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 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 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 explorer and activity explorer
- Describe sensitivity labels
- Describe Data Loss Prevention (DLP)
- Describe Records Management
- Describe Retention Policies and Retention Labels

## **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 Microsoft Purview unified data governance solution