Study guide for Exam SC-100: Microsoft Cybersecurity Architect

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
Review the skills measured as of May 5, 2023	This list represents the skills measured AFTER the date provided. Study this list if you plan to take the exam AFTER that date.
Review the skills measured prior to May 5, 2023	Study this list of skills if you take your exam PRIOR to the date provided.
Change log	You can go directly to the change log if you want to see the changes that will be made on the date provided.
How to earn the certification	Some certifications only require passing one exam, while others require passing multiple exams.
Certification renewal	Microsoft associate, expert, and specialty certifications expire annually. You can renew by passing a **free** online assessment on Microsoft Learn.
Your Microsoft Learn profile	Connecting your certification profile to Learn allows you to schedule and renew exams and share and print certificates.
Passing score	A score of 700 or greater is required to pass.
Exam sandbox	You can explore the exam environment by visiting our exam sandbox.
Request accommodations	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
Take a practice test	Are you ready to take the exam or do you need to study a bit more?

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. 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

Candidates for this exam are Microsoft cybersecurity architects who translate a cybersecurity strategy into capabilities that protect the assets, business, and operations of an organization. They design, guide the implementation of, and maintain security solutions that follow Zero Trust principles and best practices, including security strategies for identity, devices, data, applications, network, infrastructure, and DevOps. They also design solutions for Governance and Risk Compliance (GRC), security operations, and security posture management.

Cybersecurity architects continuously collaborate with leaders and practitioners in IT security, privacy, and other roles across an organization to plan and implement a cybersecurity strategy that meets the business needs of an organization.

Candidates for this exam have experience implementing or administering solutions in the following areas: identity and access, platform protection, security operations, data security, application security, and hybrid and multicloud infrastructures. They should have expert skills in at least one of those areas. They should have experience designing security solutions that include Microsoft security technologies.

To earn the Microsoft Cybersecurity Architect certification, candidates must also pass one of the following exams: SC-200, SC-300, AZ-500, or MS-500. We strongly recommend that you do this before taking this exam.

- Design solutions that align with security best practices and priorities (20–25%)
- Design security operations, identity, and compliance capabilities (30–35%)
- Design security solutions for infrastructure (20–25%)
- Design security solutions for applications and data (20–25%)

Design solutions that align with security best practices and priorities (20–25%)

Design a resiliency strategy for ransomware and other attacks based on Microsoft Security Best Practices

- Design a security strategy to support business resiliency goals, including identifying and prioritizing threats to business-critical assets
- Design solutions that align with Microsoft ransomware best practices, including backup, restore, and privileged access
- Design configurations for secure backup and restore by using Azure Backup for hybrid and multicloud environments
- Design solutions for security updates

Design solutions that align with the Microsoft Cybersecurity Reference Architectures (MCRA) and Microsoft cloud security benchmark (MCSB)

- Design solutions that align with best practices for cybersecurity capabilities and controls
- Design solutions that align with best practices for protecting against insider and external attacks
- Design solutions that align with best practices for Zero Trust security, including the Zero Trust Rapid Modernization Plan

Design solutions that align with the Microsoft Cloud Adoption Framework for Azure and the Azure Well-Architected Framework

- Design a new or evaluate an existing strategy for security and governance based on the CAF and the Well-Architected Framework
- Recommend solutions for security and governance based on the the Microsoft Cloud Adoption Framework for Azure and the Well-Architected Framework
- Design solutions for implementing and governing security by using an Azure landing zone
- Design a DevSecOps process

Design security operations, identity, and compliance capabilities (30–35%)

Design solutions for security operations

- Develop security operations capabilities to support a hybrid or multicloud environment
- Design a solution for centralized logging and auditing
- Design a solution for security information and event management (SIEM), including Microsoft Sentinel
- Design a solution for detection and response that includes extended detection and response (XDR)
- Design a solution for security orchestration automated response (SOAR), including Microsoft Sentinel and Microsoft Defender
- Design and evaluate security workflows, including incident response, threat hunting, incident management, and threat intelligence
- Design and evaluate threat detection coverage by using MITRE ATT&CK

Design solutions for identity and access management

- Design a solution for access to software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), hybrid/on-premises, and multicloud resources, including identity, networking, and application controls
- Design a solution for Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra, including hybrid and multicloud environments
- Design a solution for external identities, including B2B, B2C, and decentralized identities
- Design a modern authentication and authorization strategy, including Conditional Access, continuous access evaluation, threat intelligence integration, and risk scoring
- Validate the alignment of Conditional Access policies with a Zero Trust strategy
- Specify requirements to secure Active Directory Domain Services (AD DS)
- Design a solution to manage secrets, keys, and certificates

Design solutions for securing privileged access

- Design a solution for assigning and delegating privileged roles by using the enterprise access model
- Design an identity governance solution, including Privileged Identity Management (PIM), Privileged Access Management (PAM), privileged entitlement management, and access reviews
- Design a solution for securing the administration of cloud tenants, including SaaS and multicloud infrastructure and platforms
- Design a solution for cloud infrastructure entitlement management that includes Microsoft Entra Permissions Management
- Design a solution for Privileged Access Workstation (PAW) and bastion services

Design solutions for regulatory compliance

- Translate compliance requirements into a security solution
- Design a solution to address compliance requirements by using Microsoft Purview risk and compliance solutions
- Design a solution to address privacy requirements, including Microsoft Priva
- Design Azure Policy solutions to address security and compliance requirements
- Evaluate infrastructure compliance by using Microsoft Defender for Cloud

Design security solutions for infrastructure (20–25%)

Design solutions for security posture management in hybrid and multicloud environments

- Evaluate security posture by using MCSB
- Evaluate security posture by using Defender for Cloud
- Evaluate security posture by using Microsoft Secure Score
- Design integrated security posture management and workload protection solutions in hybrid and multicloud environments, including Defender for Cloud
- Design cloud workload protection solutions that use Defender for Cloud, such as Microsoft Defender for Servers, Microsoft Defender for App Service, and Microsoft Defender for SQL
- Design a solution for integrating hybrid and multicloud environments by using Azure Arc
- Design a solution for Microsoft Defender External Attack Surface Management (Defender EASM)

Design solutions for securing server and client endpoints

- Specify security requirements for servers, including multiple platforms and operating systems
- Specify security requirements for mobile devices and clients, including endpoint protection, hardening, and configuration
- Specify security requirements for IoT devices and embedded systems
- Design a solution for securing operational technology (OT) and industrial control systems (ICS) by using Microsoft Defender for IoT
- Specify security baselines for server and client endpoints
- Design a solution for secure remote access

Specify requirements for securing SaaS, PaaS, and IaaS services

- Specify security baselines for SaaS, PaaS, and IaaS services
- Specify security requirements for IoT workloads
- Specify security requirements for web workloads, including Azure App Service
- Specify security requirements for containers
- Specify security requirements for container orchestration

Design security solutions for applications and data (20–25%)

Design solutions for securing Microsoft 365

- Evaluate security posture for productivity and collaboration workloads by using metrics, including Secure Score and Defender for Cloud secure score
- Design a Microsoft 365 Defender solution
- Design secure configurations and operational practices for Microsoft 365 workloads and data

Design solutions for securing applications

- Evaluate the security posture of existing application portfolios
- Evaluate threats to business-critical applications by using threat modeling
- Design and implement a full lifecycle strategy for application security
- Design and implement standards and practices for securing the application development process
- Map technologies to application security requirements
- Design a solution for workload identity to authenticate and access Azure cloud resources
- Design a solution for API management and security
- Design a solution for secure access to applications, including Azure Web Application Firewall (WAF) and Azure Front Door

Design solutions for securing an organization's data

- Design a solution for data discovery and classification by using Microsoft Purview data governance solutions
- Specify priorities for mitigating threats to data
- Design a solution for protection of data at rest, data in motion, and data in use
- Design a security solution for data in Azure workloads, including Azure SQL, Azure Synapse Analytics, and Azure Cosmos DB
- Design a security solution for data in Azure Storage
- Design a security solution that includes Microsoft Defender for Storage and Defender for SQL

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
Get trained	Choose from self-paced learning paths and modules or take an instructor-led course
Find documentation	Microsoft security documentation

Study resources	Links to learning and documentation
	Microsoft Cybersecurity Reference Architectures Microsoft Defender for Cloud documentation Zero Trust Guidance Center Governance, risk, and compliance in Azure
Ask a question	Microsoft Q&A | Microsoft Docs
Get community support	Security, compliance, and identity community hub
Follow Microsoft Learn	Microsoft Learn - Microsoft Tech Community
Find a video	Exam Readiness Zone Browse other Microsoft Learn shows

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 as of May 5, 2023	Changes
Audience profile		Major
Design a Zero Trust strategy and architecture		Deleted
Build an overall security strategy and architecture		Removed
Design a security operations strategy		Removed
Design an identity security strategy		Removed
Evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies		Deleted
Design a regulatory compliance strategy		Removed

Skill area prior to May 5, 2023	Skill area as of May 5, 2023	Changes
Evaluate security posture and recommend technical strategies to manage risk		Removed
Design security for infrastructure	**Design security solutions for infrastructure**	% of exam increased
Design a strategy for securing server and client endpoints	Design solutions for securing server and client endpoints	Minor
Design a strategy for securing PaaS, IaaS, and SaaS services	Specify requirements for securing SaaS, PaaS, and IaaS services	Major
	Design solutions for security posture management in hybrid and multi-cloud environments	Added
Design a strategy for data and applications	**Design security solutions for applications and data**	Minor
Specify security requirements for applications	Design solutions for securing applications	Major
Design a strategy for securing data	Design solutions for securing an organization's data	Major
	Design solutions for securing Microsoft 365	New
Recommend security best practices and priorities	**Design solutions that align with security best practices and priorities**	Minor
Recommend security best practices by using the Microsoft Cybersecurity Reference Architecture (MCRA) and Azure Security Benchmarks	Design solutions that align with the Microsoft Cybersecurity Reference Architecture (MCRA) and Microsoft cloud security benchmark (MCSB)	Minor
Recommend a secure methodology by using the Cloud Adoption Framework (CAF)	Design solutions that align with the Cloud Adoption Framework (CAF) and Well-Architected Framework (WAF)	Minor
Recommend a ransomware strategy by using Microsoft Security Best Practices	Design a resiliency strategy for ransomware and other attacks based on Microsoft Security Best Practices	Minor
	Design security operations, identity, and compliance capabilities	New

Skill area prior to May 5, 2023	Skill area as of May 5, 2023	Changes
	Design solutions for security operations	Added
	Design solutions for identity and access management	Added
	Design solutions for securing privileged access	New
	Design solutions for regulatory compliance	Added

Skills measured prior to May 5, 2023

Audience profile

The Microsoft cybersecurity architect has subject matter expertise in designing and evolving the cybersecurity strategy to protect an organization's mission and business processes across all aspects of the enterprise architecture. The cybersecurity architect designs a Zero Trust strategy and architecture, including security strategies for data, applications, access management, identity, and infrastructure. The cybersecurity architect also evaluates Governance Risk Compliance (GRC) technical strategies and security operations strategies.

The cybersecurity architect continuously collaborates with leaders and practitioners in IT security, privacy, and other roles across an organization to plan and implement a cybersecurity strategy that meets the business needs of an organization.

A candidate for this certification should have advanced experience and knowledge in a wide range of security engineering areas including identity and access, platform protection, security operations, securing data and securing applications. They should also have experience with hybrid and cloud implementations.

To earn the Microsoft Cybersecurity Architect certification, candidates must also pass one of the following exams: SC-200, SC-300, AZ-500, or MS-500. We strongly recommend that you do this before taking this exam.

- Design a Zero Trust strategy and architecture (30–35%)
- Evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies (10–15%)
- Design security for infrastructure (10–15%)
- Design a strategy for data and applications (15–20%)
- Recommend security best practices and priorities (20–25%)

Design a Zero Trust strategy and architecture (30–35%)

Build an overall security strategy and architecture

- Identify the integration points in a security architecture by using Microsoft Cybersecurity Reference Architecture (MCRA)
- Translate business goals into security requirements
- Translate security requirements into technical capabilities, including security services, security products, and security processes
- Design security for a resiliency strategy
- Integrate a hybrid or multi-tenant environment into a security strategy
- Develop a technical governance strategy for security

Design a security operations strategy

- Design a logging and auditing strategy to support security operations
- Develop security operations to support a hybrid or multi-cloud environment
- Design a strategy for SIEM and SOAR
- Evaluate security workflows
- Evaluate a security operations strategy for incident management lifecycle
- Evaluate a security operations strategy for sharing technical threat intelligence

Design an identity security strategy

- Design a strategy for access to cloud resources
- Recommend an identity store (tenants, B2B, B2C, hybrid)
- Recommend an authentication strategy
- Recommend an authorization strategy
- Design a strategy for conditional access
- Design a strategy for role assignment and delegation
- Design security strategy for privileged role access to infrastructure including identity-based firewall rules and Privileged Identity Management (PIM) in Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra
- Design security strategy for privileged activities including PAM, entitlement management, cloud tenant administration

Evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies (10–15%)

Design a regulatory compliance strategy

- Interpret compliance requirements and translate into specific technical capabilities (new or existing)
- Evaluate infrastructure compliance by using Microsoft Defender for Cloud
- Interpret compliance scores and recommend actions to resolve issues or improve security

- Design implementation of Azure Policy
- Design for data residency requirements
- Translate privacy requirements into requirements for security solutions

Evaluate security posture and recommend technical strategies to manage risk

- Evaluate security posture by using Azure Security Benchmark
- Evaluate security posture by using Microsoft Defender for Cloud
- Evaluate security posture by using Secure Scores
- Evaluate security posture of cloud workloads
- Design security for an Azure Landing Zone
- Interpret technical threat intelligence and recommend risk mitigations
- Recommend security capabilities or controls to mitigate identified risks

Design security for infrastructure (10–15%)

Design a strategy for securing server and client endpoints

- Specify security baselines for server and client endpoints
- Specify security requirements for servers, including multiple platforms and operating systems
- Specify security requirements for mobile devices and clients, including endpoint protection, hardening, and configuration
- Specify requirements to secure Active Directory Domain Services
- Design a strategy to manage secrets, keys, and certificates
- Design a strategy for secure remote access
- Design a strategy for securing privileged access

Design a strategy for securing SaaS, PaaS, and IaaS services

- Specify security baselines for SaaS, PaaS, and IaaS services
- Specify security requirements for IoT workloads
- Specify security requirements for data workloads, including Azure SQL, Azure Synapse Analytics, and Azure Cosmos DB
- Specify security requirements for web workloads, including Azure App Service
- Specify security requirements for storage workloads, including Azure Storage
- Specify security requirements for containers
- Specify security requirements for container orchestration

Design a strategy for data and applications (15–20%)

Specify security requirements for applications

- Specify priorities for mitigating threats to applications
- Specify a security standard for onboarding a new application
- Specify a security strategy for applications and APIs

Design a strategy for securing data

- Specify priorities for mitigating threats to data
- Design a strategy to identify and protect sensitive data
- Specify an encryption standard for data at rest and in motion

Recommend security best practices and priorities (20–25%)

Recommend security best practices by using the Microsoft Cybersecurity Reference Architecture (MCRA) and Azure Security Benchmarks

- Recommend best practices for cybersecurity capabilities and controls
- Recommend best practices for protecting from insider and external attacks
- Recommend best practices for Zero Trust security
- Recommend best practices for Zero Trust Rapid Modernization Plan

Recommend a secure methodology by using the Cloud Adoption Framework (CAF)

- Recommend a DevSecOps process
- Recommend a methodology for asset protection
- Recommend strategies for managing and minimizing risk

Recommend a ransomware strategy by using Microsoft Security Best Practices

- Plan for ransomware protection and extortion-based attacks (i.e., Backup and recovery, limit scope)
- Protect assets from ransomware attacks
- Recommend Microsoft ransomware best practices