Study Guide
Exam SC-100: Microsoft Cybersecurity Architect

Quick navigation

Purpose of this document
Certification
  Certification renewal
About the exam
  Passing score
  What to expect on the exam
Prepare to take the exam
  Request accommodations
  Objective domain: skills the exam measures
Skills measured
  Functional groups
Corresponding learning paths and modules
Additional study resources
Purpose of this document

This study guide should help you understand what to expect on Exam SC-100: Microsoft Cybersecurity Architect 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.

Certification

Certification renewal

Once you earn your certification, don’t let it expire. When you have an active certification that’s expiring within six months, you should renew it—at no cost—by passing a renewal assessment on Microsoft Learn. Remember to renew your certification annually, if you want to retain it.

To identify which certifications are available for you to renew, visit your Certifications in your Microsoft Learn profile:

- Ensure your certification profile is connected to your Learn profile.
- Expect an email that directs you to the applicable assessment that you must pass on Microsoft Learn. You’ll receive this email as soon as you have a certification that you’re eligible to renew.
- When you pass an online assessment, your certification will extend by one year from the current expiration date.
- To help prepare for the assessment, explore the collection of free modules on the certification renewal page.

About the exam

Exam SC-100: Microsoft Cybersecurity Architect is required to earn the Microsoft Cybersecurity Architect Expert certification.

This exam measures your ability to accomplish the following technical tasks: design a Zero Trust strategy and architecture; evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies; design security for infrastructure; and design a strategy for data and applications.

As an exam candidate, you 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.

Passing score

A passing score is 700. Learn more about exam scoring and score reports.
What to expect on the exam
Are you new to Microsoft certification exams? You can explore the exam environment by visiting our exam sandbox. We created the sandbox so you have an opportunity to experience an exam before you take it. In the sandbox, you can interact with different question types, such as build list, case studies, and others that you might encounter in the user interface when you take an exam. Additionally, it includes the introductory screens, instructions, and help topics related to the different types of questions that your exam might include. It also includes the non-disclosure agreement that you must accept before you can launch the exam.

Prepare to take the exam
There are several points to consider, or pursue, as you prepare for an exam. The following sections detail those points.

Request accommodations
We’re committed to ensuring all learners are set up for success. If you use assistive devices, require extra time, or need modification to any part of the exam experience, you can request an accommodation. We encourage you to learn more about available accommodations and how to obtain them by visiting this page.

Objective domain: skills the exam measures
The English language version of this exam was released on June 30, 2022.

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

**Functional groups**

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

**Build an overall security strategy and architecture**
- Identify the integration points in an 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 and governance strategy for traffic filtering and segmentation

**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**
Note: includes hybrid and multi-cloud
- 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, Azure PIM
- Design security strategy for privileged activities including PAM, entitlement management, cloud tenant administration
Evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies (20–25%)

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 benchmarks (including Azure security benchmarks, ISO 2701, etc.)
- 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 (20–25%)

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 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 SQL, Azure SQL Database, Azure Synapse, 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 (20–25%)  

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

Corresponding learning paths and modules

The design of learning paths and modules should teach you how to perform a role and will help you study for the applicable exam. However, learning paths aren’t always in the same order as an exam’s “skills measured” list. Therefore, we’ve created a convenient table that links the skills measured to specific paths and modules.

<table>
<thead>
<tr>
<th>Exam skills measured</th>
<th>Links to learning paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design a Zero Trust strategy and architecture (30–35%)</td>
<td>SC-100: Design a Zero Trust strategy and architecture</td>
</tr>
<tr>
<td></td>
<td>- Build an overall security strategy and architecture</td>
</tr>
<tr>
<td></td>
<td>- Design a security operations strategy</td>
</tr>
<tr>
<td></td>
<td>- Design an identity security strategy</td>
</tr>
<tr>
<td>Evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies (20–25%)</td>
<td>SC-100: Evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies</td>
</tr>
<tr>
<td></td>
<td>- Evaluate a regulatory compliance strategy</td>
</tr>
<tr>
<td></td>
<td>- Evaluate security posture and recommend technical strategies to manage risk</td>
</tr>
<tr>
<td>Design security for infrastructure (20–25%)</td>
<td>SC-100: Design security for infrastructure</td>
</tr>
<tr>
<td></td>
<td>- Understand architecture best practices and how they are changing with the Cloud</td>
</tr>
<tr>
<td></td>
<td>- Design a strategy for securing server and client endpoints</td>
</tr>
<tr>
<td></td>
<td>- Design a strategy for securing PaaS, IaaS, and SaaS services</td>
</tr>
</tbody>
</table>
Exam SC-100: Microsoft Cybersecurity Architect

### Exam skills measured

**Design a strategy for data and applications (20–25%)**

- SC-100: Design a strategy for data and applications
  - Specify security requirements for applications
  - Design a strategy for securing data

### Additional study resources

We offer several resources to help you prepare for the exam and stay current and engaged with the Microsoft Azure community. These resources range from formal training to blogs and even interviews with Microsoft team members.

<table>
<thead>
<tr>
<th>Study resource link</th>
<th>Resource description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Course SC-100T00: Microsoft Cybersecurity Architect</strong></td>
<td>Take a four-day, instructor-led course that prepares you with the background to design and evaluate cybersecurity strategies in the following areas: Zero Trust, Governance Risk Compliance (GRC), security operations (SecOps), and data and applications. You will also learn how to design and architect solutions using zero trust principles and specify security requirements for cloud infrastructure in different service models (SaaS, PaaS, IaaS).</td>
</tr>
<tr>
<td>**Microsoft security documentation - Security documentation</td>
<td>Microsoft Docs**</td>
</tr>
<tr>
<td><strong>Security, compliance, and identity community hub</strong></td>
<td>Welcome to the Security, Compliance, and Identity Community! Connect and discuss the latest news, updates, and best practices with Microsoft professionals and peers.</td>
</tr>
<tr>
<td><strong>Inside Azure for IT</strong></td>
<td>Welcome to the Microsoft 365 Blog! Learn best practices, news, and trends directly from the Microsoft 365 team.</td>
</tr>
<tr>
<td><strong>Well-Architected: The Backstage Tour</strong></td>
<td>Reliability, security, cost optimization, operational excellence, and performance efficiency—not easy to tackle when it comes to your cloud workloads. This is where the Azure Well-Architected Framework comes into the picture. In this pre-recorded event we take you behind the scenes at Azure where you will get five brief peeks at how we power the features that address each of these pillars of the Azure Well-Architected Framework. Not only will you learn how things</td>
</tr>
</tbody>
</table>
work behind the curtain, but you’ll also take away some tips and tricks you won’t find anywhere else to help with these subjects.

<table>
<thead>
<tr>
<th>Study resource link</th>
<th>Resource description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Azure Security Benchmark introduction</strong></td>
<td>Microsoft has found that using security benchmarks can help you quickly secure cloud deployments. Benchmark recommendations from your cloud service provider give you a starting point for selecting specific security configuration settings in your environment and allow you to quickly reduce risk to your organization.</td>
</tr>
</tbody>
</table>