SC-100: Microsoft Azure Certified Cybersecurity Architect Expert Exam Study Guide

March 7, 2023 by manish

☆☆☆☆☆ Rate this post

Are you considering taking the SC-100 Exam: Microsoft Cybersecurity Architect? Then this guide is for you if you are interested in becoming a Microsoft Cyber Security Architect.

SC-100 certifications are designed for people who've got a lot of experience and knowledge in security engineering specifically identity and access, platform security, security operations, data security, application security, and hybrids.

In this certification, you learn how to design and implement security solutions

in hybrid and cloud-only environments and become a Microsoft Cybersecurity Architect.

Here, we'll look at SC-100 certification in detail, as well as test policy and prerequisites, and a Microsoft Cybersecurity Architect's role and responsibilities.

Table of Contents

SC-100 Certification Overview

To keep up with today's demanding IT environments, Microsoft is constantly evolving its learning programs. Learning at Microsoft is constantly evolving so you can master new skills, prove your expertise to employers, and get the recognition and opportunities you deserve.

SC-100 certification is designed for candidates who have knowledge of different aspects of Microsoft Security and are able to design and implement security solutions.

It is an advanced-level certificate exam offered by Microsoft Azure. It tests your ability to design and implement Microsoft security solutions based on enterprise architecture.

You'll be tested on Azure security, identity and access management, data protection, and more in this SC-100 exam.

Are you new to Azure Cloud? Do check out our blog post on the Microsoft Azure Certification Path 2023 and choose the best certification for you.

Who Is Microsoft Certified Cybersecurity Architect Expert?

The Microsoft cybersecurity architect knows how to design and evolve cybersecurity strategies to protect an organization's mission and business processes.

Cybersecurity architects design Zero Trust strategies and architectures for data, applications, access management, identity, and infrastructure.

Additionally, the cybersecurity architect evaluates Governance Risk Compliance (GRC) technical strategies.

They plan and implement a cybersecurity strategy that meets an organization's business needs in collaboration with leaders and practitioners across IT security, privacy, and other disciplines.

Who Is This Certification For?

- For architects who want to validate their security strategies to protect an organization's processes and infrastructure, the SC-100 is a good choice.
- Additionally, it involves designing a zero-trust strategy, assessing Governance Risk Compliance, and so on.
- This exam will be a perfect fit for those in or seeking to move into information security roles.
- If you have a strong understanding of security architectures and concepts, you can successfully complete the SC-100 exam even if you have no prior experience with cybersecurity.

Why SC-100 Certification?

Taking the SC-100 exam will show your organization or potential employer that you are capable of becoming a successful Microsoft Cybersecurity Architect. When you apply for jobs, SC-100 enables you to stand out from the crowd.

With the SC-100 certification, you will learn how to construct cybersecurity strategies, develop zero trust strategies, manage access, etc.

Also, there are many reasons to take the SC-100 exam, including:

- Provides assistance in designing cybersecurity architecture elements
- Assists in validating skills and knowledge in Governance Risk Compliance (GRC) technologies
- Validates skills for Zero trust strategy creation.

Microsoft Cybersecurity Architect Roles & Responsibilities

Among the responsibilities and roles of the Microsoft Cybersecurity Architect (SC-100) are:

- Plan and build a Zero Trust strategy, such as security strategies for applications, data, access management, identity, and infrastructure.
- Technical and operational assessment of Governance Risk Compliance (GRC)
- Work with organizations' IT security, privacy, and other leaders and practitioners
- Prepare and implement an organization's cybersecurity strategy.

SC-100 Exam Details

Exam Name	Passing Marks
SC-100: Microsoft Certified Cybersecurity Architect Expert	700
Exam Fee	**Exam Duration**
$165	120 Minutes
Exam Validity	**Exam Languages**
1 Year	English, Japanese, Chinese (Simplified), Korean, German, French, Spanish, Portuguese (Brazil), Chinese (Traditional), Italian
Total Questions	**Exam Type**
40-60 Questions	Multiple-choice and Multiple response questions

SC-100 Exam Skills Measured

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%

How to Register for SC 100 Certification Exam

You can register for the Microsoft Certified Cybersecurity Architect Expert Exam (SC-100) by going to the Official Microsoft Page.

Schedule exam

Exam SC-100: Microsoft Cybersecurity Architect

United States

Languages: English, Japanese, Chinese (Simplified), Korean, German, French, Spanish, Portuguese (Brazil), Chinese (Traditional), Italian
Retirement date: none

$165 USD*

Price based on the country or region in which the exam is proctored.

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; design a strategy for data and applications; and recommend security best practices and priorities.

Schedule exam >

MeasureUp practice test for Microsoft Cybersecurity Architect
All objectives of the exam are covered in depth so you'll be ready for any question on the exam.

⊕ Add

Prerequisite for SC 100 Certification

The following prerequisites are provided by Microsoft to help you prepare for the SC-100 exam:

- The candidate should have advanced experience and knowledge in areas like identity and access, platform protection, security operations,

and securing data and apps.

- Candidates must have experience implementing hybrid and cloud solutions.
- Before attempting the SC-100 exam, the candidate must earn the SC-200, SC-300, AZ-500 or MS-500 certifications.

SC-100 Study Guide

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

Build an overall security strategy and architecture

- Identify the integration points in architecture by using Microsoft Cybersecurity Reference Architecture (MCRA)
  - Microsoft Cybersecurity Reference Architectures
  - Cybersecurity Reference Architecture: Security for a Hybrid Enterprise
- Translate business goals into security requirements
  - How to organize your security team: The evolution of cybersecurity roles and responsibilities
  - Security governance
- Translate security requirements into technical capabilities, including security services, security products, and security processes
  - Introduction to Azure security
  - Azure security technical capabilities
- Design security for a resiliency strategy
  - Define a security strategy
- Integrate a hybrid or multi-tenant environment into a security strategy
  - Security in a hybrid workload
- Develop a technical and governance strategy for traffic filtering and segmentation
  - Filter network traffic with a network security group using the Azure portalBuild a cloud governance strategy on AzureSegmentation

strategies
- Implement network segmentation patterns on Azure

Design a security operations strategy

- Design a logging and auditing strategy to support security operations
  - Design a Log Analytics workspace architecture
  - Azure security logging and auditing
- Develop security operations to support a hybrid or multi-cloud environment
  - Protecting multi-cloud environments with Azure Security Center
  - Protect multi-cloud workloads with new Azure security innovations
  - Monitor hybrid security using Microsoft Defender for Cloud and Microsoft Sentinel
- Design a strategy for SIEM and SOAR
  - MICROSOFT AZURE SENTINEL
- Evaluate security workflows
  - Automate responses to Microsoft Defender for Cloud triggers
- Evaluate a security operations strategy for incident management lifecycle
  - Security Control V2: Incident Response
- Evaluate a security operations strategy for sharing technical threat intelligence
  - Microsoft uses threat intelligence to protect, detect, and respond to threats

Design an identity security strategy

- Design a strategy for access to cloud resources
  - Designing your cloud strategy to maximize value on Azure
  - Azure identity and access management considerations
- 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 (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 risk

Design security for infrastructure (10–15%)

- Design a strategy for securing server and client endpoints
  - Specify security baselines for server and client endpointsSpecify security requirements for servers, including multiple platforms and operating systemsSpecify security requirements for mobile devices and clients, including endpoint protection, hardening, and configurationSpecify requirements to secure Active Directory Domain ServicesDesign a strategy to manage secrets, keys, and certificatesDesign 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 servicesSpecify security requirements for IoT workloadsSpecify security requirements for data workloads, including Azure SQL, Azure Synapse Analytics, and Azure Cosmos DBSpecify security requirements for web workloads, including Azure App ServiceSpecify security requirements for storage workloads, including Azure StorageSpecify 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 applicationsSpecify 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 dataDesign 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 controlsRecommend best practices for protecting from insider and external attacksRecommend 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 processRecommend 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 (ie. Backup and recovery, limit scope)Protect assets from ransomware attacks
  - Recommend Microsoft ransomware best practices

SC-100 Exam Retake Policy

- Those who fail the exam for the first time have to wait 24 hours before retaking it. On the certification dashboard, they can reschedule the exam during this period.
- The second time they take the exam, they may be asked to wait at least 14 days before taking it again.
- There is a 14-day waiting period between the third and fourth attempts and between the fourth and fifth attempts.
- On the other hand, candidates are only allowed to take the test five times per year. Also, the 12-month period begins upon the first attempt.

Conclusion

To conclude, the SC-100 certification is a great step toward becoming a Microsoft Cybersecurity Architect.

You can demonstrate your expertise in identity and access, platform security, security operations, data security, and application security in this certification, which emphasizes designing and implementing security solutions in hybrid and cloud-only environments.

With the SC-100 exam, you will be able to demonstrate your knowledge and skills in Governance Risk Compliance (GRC) technologies.

It is highly recommended that you pursue the SC-100 certification if you wish to take your cybersecurity career to the next level.

FAQs

1. Is the SC-100 exam hard?

SC-100 is a challenging exam, even though it doesn't get into technical details. It's crucial to understand how Azure solutions integrate with security if you want to do well on the exam.

2. How is the SC-100 exam structured?

Questions on the SC-100 exam usually follow a variety of formats, including single-answer, multiple-choice, sequence-based, drag-and-drop, and review-and-drag-and-drop questions. 120 minutes are allocated for the entire test.

### 3. Is there any retirement data for the SC-100 exam?

There is no retirement date for this exam. You can attend this exam whenever it is convenient for you.

4. What is the validation period for this SC-100 certification?

It is valid for one year after passing the exam, and then recertification occurs. Also, certifications are updated based on performance.

Related Articles

- AZ-500 Exam Study Guide
- AZ-204 Exam Study Guide
- SC-900 Exam Study Guide
- AI-900 Exam Study Guide
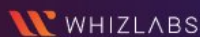
Leave a Comment

Name *

Email *

☐ Save my name, email, and website in this browser for the next time I comment.
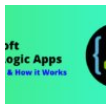
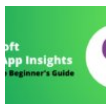**Post Comment**

Recent Posts

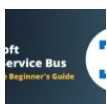Microsoft Azure Certification Path in 2023 | Azure Certification Roadmap for Beginners

Azure Storage Explorer: Download, Install, and Setup Overview

What are Azure Logic Apps: Components, Advantages and How it Works

Microsoft Azure Application Insights: A Complete Beginners Guide

Microsoft Azure Service Bus: A Complete Beginners Guide