EDUSUM
#1 Online Certification Guide

MICROSOFT SC-100

Microsoft Cybersecurity Architect Certification Questions & Answers

Exam Summary – Syllabus –Questions

SC-100
Microsoft Certified - Cybersecurity Architect Expert
40-60 Questions Exam – 700 / 1000 Cut Score – Duration of 120 minutes

Table of Contents:

Know Your SC-100 Certification Well:

The SC-100 is best suitable for candidates who want to gain knowledge in the Microsoft Security Compliance and Identity. Before you start your SC-100 preparation you may struggle to get all the crucial Cybersecurity Architect materials like SC-100 syllabus, sample questions, study guide.

But don't worry the SC-100 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the SC-100 syllabus?
- How many questions are there in the SC-100 exam?
- Which Practice test would help me to pass the SC-100 exam at the first attempt?

Passing the SC-100 exam makes you Microsoft Certified - Cybersecurity Architect Expert. Having the Cybersecurity Architect certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

Microsoft SC-100 Cybersecurity Architect Certification Details:

Exam Name	Microsoft Certified - Cybersecurity Architect Expert
Exam Code	SC-100
Exam Price	$165 (USD)
Duration	120 mins
Number of Questions	40-60
Passing Score	700 / 1000
Books / Training	**Course SC-100T00: Microsoft Cybersecurity Architect**
Schedule Exam	**Pearson VUE**
Sample Questions	**Microsoft Cybersecurity Architect Sample Questions**
Practice Exam	**Microsoft SC-100 Certification Practice Exam**

SC-100 Syllabus:

Topic	Details
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	- 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,

Topic	Details
	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

Topic	Details
	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

Microsoft SC-100 Sample Questions:

Question: 1

You have a customer that has a Microsoft 365 subscription and an Azure subscription. The customer has devices that run either Windows, iOS, Android, or macOS. The Windows devices are deployed on-premises and in Azure.
You need to design a security solution to assess whether all the devices meet the customer's compliance rules. What should you include in the solution?

a) Microsoft Information Protection
b) Microsoft Defender for Endpoint
c) Microsoft Sentinel
d) Microsoft Endpoint Manager

Answer: d

Question: 2

You are designing the security standards for a new Azure environment. You need to design a privileged identity strategy based on the Zero Trust model. Which framework should you follow to create the design?

a) Microsoft Security Development Lifecycle (SDL)
b) Enhanced Security Admin Environment (ESAE)
c) Rapid Modernization Plan (RaMP)
d) Microsoft Operational Security Assurance (OSA)

Answer: b

Question: 3

You have an Azure subscription that contains several storage accounts. The storage accounts are accessed by legacy applications that are authenticated by using access keys. You need to recommend a solution to prevent new applications from obtaining the access keys of the storage accounts.
The solution must minimize the impact on the legacy applications. What should you include in the recommendation?

a) Apply read-only locks on the storage accounts.
b) Set the AllowBlobPublicAcccss property to false.
c) Configure automated key rotation.
d) Set the AllowSharcdKeyAccess property to false.

Answer: a

Question: 4

You have a Microsoft 365 E5 subscription. You need to recommend a solution to add a watermark to email attachments that contain sensitive data. What should you include in the recommendation?

- a) insider risk management
- b) Microsoft Defender for Cloud Apps
- c) Microsoft Information Protection
- d) Azure Purview

Answer: b

Question: 5

A customer follows the Zero Trust model and explicitly verifies each attempt to access its corporate applications. The customer discovers that several endpoints are infected with malware. The customer suspends access attempts from the infected endpoints. The malware is removed from the end point.
Which two conditions must be met before endpoint users can access the corporate applications again?
Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- a) Microsoft Defender for Endpoint reports the endpoints as compliant.
- b) Microsoft Intune reports the endpoints as compliant.
- c) A new Azure Active Directory (Azure AD) Conditional Access policy is enforced.
- d) The client access tokens are refreshed.

Answer: c, d

Question: 6

To meet the application security requirements, which two authentication methods must the applications support?
Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- a) Security Assertion Markup Language (SAML)
- b) certificate-based authentication
- c) NTLMv2
- d) Kerberos

Answer: a, b

Question: 7

You have an Azure subscription that has Microsoft Defender for Cloud enabled. Suspicious authentication activity alerts have been appearing in the Workload protections dashboard. You need to recommend a solution to evaluate and remediate the alerts by using workflow automation. The solution must minimize development effort.
What should you include in the recommendation?

a) Azure Logics Apps
b) Azure Event Hubs
c) Azure Functions apps
d) Azure Monitor webhooks

Answer: c

Question: 8

You have a Microsoft 365 E5 subscription. You are designing a solution to protect confidential data in Microsoft SharePoint Online sites that contain more than one million documents. You need to recommend a solution to prevent Personally Identifiable Information (Pll) from being shared.
Which two components should you include in the recommendation?
Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

a) data loss prevention (DLP) policies
b) sensitivity label policies
c) retention label policies
d) eDiscovery cases

Answer: a, d

Question: 9

You have an Azure subscription that is used as an Azure landing zone for an application. You need to evaluate the security posture of all the workloads in the landing zone. What should you do first?

a) Enable the Defender plan for all resource types in Microsoft Defender for Cloud.
b) Configure Continuous Integration/Continuous Deployment (CI/CD) vulnerability scanning.
c) Obtain Azure Active Directory Premium Plan 2 licenses.
d) Add Microsoft Sentinel data connectors

Answer: d

Question: 10

You are creating an application lifecycle management process based on the Microsoft Security Development Lifecycle (SDL). You need to recommend a security standard for onboarding applications to Azure. The standard will include recommendations for application design, development, and deployment.

What should you include during the application design phase?

a) software decomposition by using Microsoft Visual Studio Enterprise
b) threat modeling by using the Microsoft Threat Modeling Tool
c) dynamic application security testing (DAST) by using Veracode
d) static application security testing (SAST) by using SonarQube

Answer: a

Study Guide to Crack Microsoft Cybersecurity Architect SC-100 Exam:

- Getting details of the SC-100 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the SC-100 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the Microsoft provided training for SC-100 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the SC-100 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on SC-100 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for SC-100 Certification

Make EduSum.com your best friend during your Microsoft Cybersecurity Architect exam preparation. We provide authentic practice tests for the SC-100 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual SC-100 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the SC-100 exam.

Start Online Practice of SC-100 Exam by visiting URL
https://www.edusum.com/microsoft/sc-100-microsoft-cybersecurity-architect