SC-100Q&As

Microsoft Cybersecurity Architect

Pass Microsoft SC-100 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/sc-100.html

100% Passing Guarantee
100% Money Back Assurance

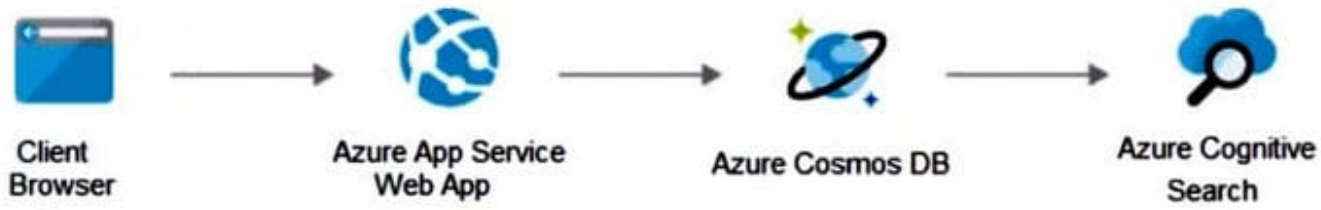
Following Questions and Answers are all new published by Microsoft Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your on-premises network contains an e-commerce web app that was developed in Angular and Node,js. The web app uses a MongoDB database. You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.

Solution: You recommend implementing Azure Front Door with Azure Web Application Firewall (WAF).

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead use solution: You recommend creating private endpoints for the web app and the database layer.

Note:

How to Use Azure Private Endpoints to Restrict Public Access to WebApps.

As an Azure administrator or architect, you are sometimes asked the question: “How can we safely deploy internal business applications to Azure App Services?”

These applications characteristically are:

Not accessible from the public internet.

Accessible from within the on-premises corporate network

Accessible via an authorized VPN client from outside the corporate network.

For such scenarios, we can use Azure Private Links, which enables private and secure access to Azure PaaS services over Azure Private Endpoints, along with the Site-to-Site VPN, Point-to-Site VPN, or the Express Route. Azure Private

Endpoint is a read-only network interface service associated with the Azure PAAS Services. It allows you to bring deployed sites into your virtual network, limiting access to them at the network level.

It uses one of the private IP addresses from your Azure VNet and associates it with the Azure App Services. These

services are called Private Link resources. They can be Azure Storage, Azure Cosmos DB, SQL, App Services Web App,

your own / partner owned services, Azure Backups, Event Grids, Azure Service Bus, or Azure Automations.

Reference: https://www.varonis.com/blog/securing-access-azure-webapps

QUESTION 2

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are designing the encryption standards for data at rest for an Azure resource.

You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.

Solution: For blob containers in Azure Storage, you recommend encryption that uses Microsoft-managed keys within an encryption scope.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Need to use customer-managed keys instead.

Note: Automated key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency. You can use rotation policy to configure rotation for each individual key. Our recommendation is to rotate encryption keys at least every two years to meet cryptographic best practices. This feature enables end-to-end zero-touch rotation for encryption at rest for Azure services with customer-managed key (CMK) stored in Azure Key Vault. Please refer to specific Azure service documentation to see if the service covers end

to-end rotation.

Reference: https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

QUESTION 3

You have an operational model based on the Microsoft Cloud Adoption Framework for Azure.

You need to recommend a solution that focuses on cloud-centric control areas to protect resources such as endpoints, databases, files, and storage accounts.

What should you include in the recommendation?

A. business resilience

B. modem access control

C. network isolation

D. security baselines in the Microsoft Cloud Security Benchmark

Correct Answer: D

Explanation:

The Microsoft cloud security benchmark (MCSB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure and your multi-cloud environment. This benchmark focuses

on cloud-centric control areas with input from a set of holistic Microsoft and industry security guidance.

Controls include:

*

Endpoint Security (ES)

Endpoint Security covers controls in endpoint detection and response, including use of endpoint detection and response (EDR) and anti-malware service for endpoints in cloud environments.

*

Data Protection (DP)

Data Protection covers control of data protection at rest, in transit, and via authorized access mechanisms, including discover, classify, protect, and monitor sensitive data assets using access control, encryption, key management and

certificate management.

*

Etc.

Reference: https://learn.microsoft.com/en-us/security/benchmark/azure/overview

QUESTION 4

Your company is preparing for cloud adoption.

You are designing security for Azure landing zones.

Which two solutions should you include in the design to ensure that preventative controls are implemented to increase the secure score? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Azure Web Application Firewall (WAF)

B. Azure AD Privileged Identity Management (PIM)

C. Microsoft Sentinel

D. Azure Firewall

E. Microsoft Defender for Cloud alerts

Correct Answer: BC

B: Azure identity and access for landing zones, Privileged Identity Management (PIM)

Use Azure AD Privileged Identity Management (PIM) to establish zero-trust and least privilege access. Map your organization\\'s roles to the minimum access levels needed. Azure AD PIM can use Azure native tools, extend current tools and

processes, or use both current and native tools as needed.

Azure identity and access for landing zones, Design recommendations include:

*

(B) Use Azure AD managed identities for Azure resources to avoid credential-based authentication. Many security breaches of public cloud resources originate with credential theft embedded in code or other text. Enforcing managed identities for programmatic access greatly reduces the risk of credential theft.

*

Etc.

C: Improve landing zone security, onboard Microsoft Sentinel You can enable Microsoft Sentinel, and then set up data connectors to monitor and protect your environment. After you connect your data sources using data connectors, you choose from a gallery of expertly created workbooks that surface insights based on your data. These workbooks can be easily customized to your needs.

Note: Landing zone security best practices

The following list of reference architectures and best practices provides examples of ways to improve landing zone security:

Microsoft Defender for Cloud: Onboard a subscription to Defender for Cloud.

Microsoft Sentinel: Onboard to Microsoft Sentinel to provide a security information event management (SIEM) and security orchestration automated response (SOAR) solution.

Secure network architecture: Reference architecture for implementing a perimeter network and secure network architecture.

Identity management and access control: Series of best practices for implementing identity and access to secure a landing zone in Azure.

Network security practices: Provides additional best practices for securing the network.

Operational security provides best practices for increasing operational security in Azure.

The Security Baseline discipline: Example of developing a governance-driven security baseline to enforce security requirements.

Incorrect:

Not E: Implementing alerts is not a preventive measure.

Reference: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/identity-access-landing-zones

https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard

QUESTION 5

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Defender for Cloud, review the secure score recommendations.

B. From Microsoft Sentinel, configure the Microsoft Defender for Cloud data connector.

C. From Defender for Cloud, review the Azure security baseline for audit report.

D. From Defender for Cloud, add a regulatory compliance standard.

Correct Answer: D

Add a regulatory standard to your dashboard

The following steps explain how to add a package to monitor your compliance with one of the supported regulatory standards.

Add a standard to your Azure resources

1.

From Defender for Cloud\\'s menu, select Regulatory compliance to open the regulatory compliance dashboard. Here you can see the compliance standards currently assigned to the currently selected subscriptions.

2.

From the top of the page, select Manage compliance policies. The Policy Management page appears.

3.

Select the subscription or management group for which you want to manage the regulatory compliance posture.

4.

To add the standards relevant to your organization, expand the Industry and regulatory standards section and select Add more standards.

5.

From the Add regulatory compliance standards page, you can search for any of the available standards:

6.

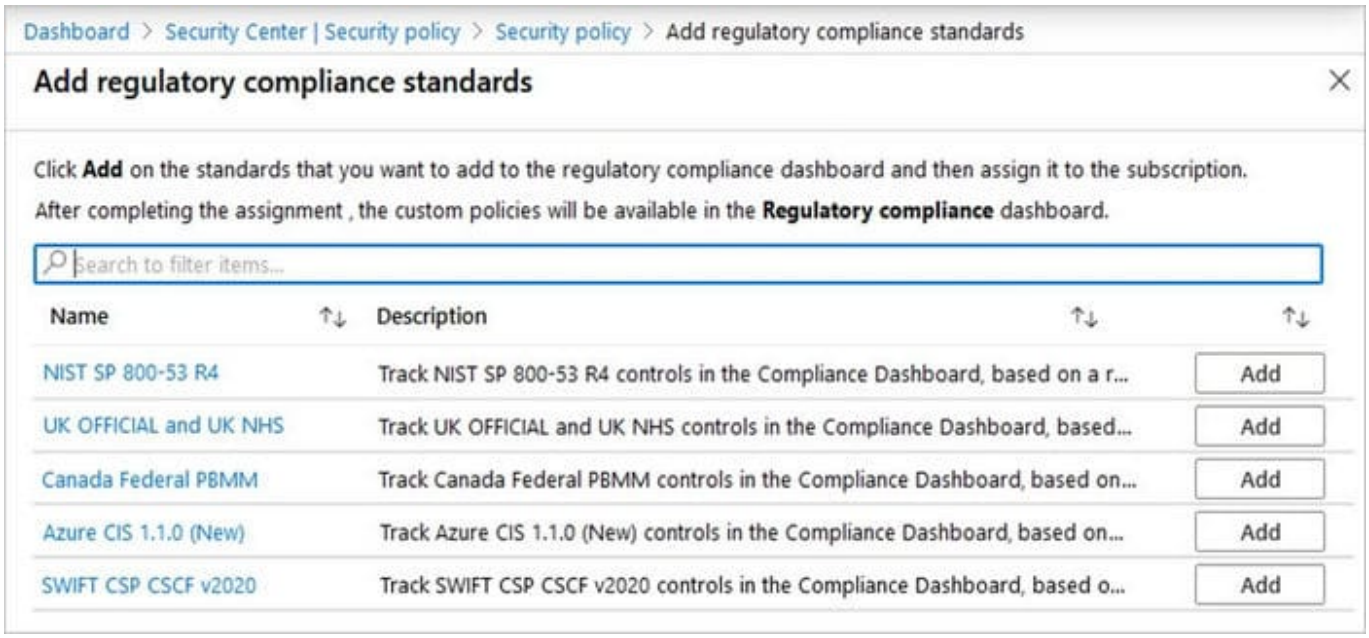
Select Add and enter all the necessary details for the specific initiative such as scope, parameters, and remediation.

7.

From Defender for Cloud\\'s menu, select Regulatory compliance again to go back to the regulatory compliance dashboard.

Your new standard appears in your list of Industry and regulatory standards.

Note: Customize the set of standards in your regulatory compliance dashboard.



Microsoft Defender for Cloud continually compares the configuration of your resources with requirements in industry standards, regulations, and benchmarks. The regulatory compliance dashboard provides insights into your compliance posture based on how you\\'re meeting specific compliance requirements. Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages

SC-100 PDF Dumps SC-100 Exam Questions SC-100 Braindumps