CSA CCSK Mock Exam

Shared by Santana on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What method can be utilized along with data fragmentation to enhance security?

Options:

A- Encryption
B- Organization
C- Knowledge management
D- IDS
E- Insulation

Answer:

E

Question 2

Question Type: MultipleChoice

What is a primary objective of cloud governance in an organization?

Options:

A- Implementing multi-tenancy and resource pooling.
B- To align cloud usage with corporate objectives
C- Simplifying scalability and automating resource management
D- Enhancing user experience and reducing latency

Answer:

B

Explanation:

The primary objective of cloud governance in an organization is to align cloud usage with corporate objectives. Cloud governance ensures that the cloud resources, services, and strategies are used effectively and efficiently, supporting the organization's overall goals and

priorities. It involves establishing policies, compliance measures, and management practices to ensure that cloud adoption and usage are aligned with business needs, security requirements, and regulatory obligations.

Implementing multi-tenancy and resource pooling is important for cloud infrastructure but is more related to the underlying technology rather than governance. Simplifying scalability and automating resource management are benefits of cloud environments, but they are more about cloud architecture and operations than governance. Enhancing user experience and reducing latency are concerns of performance optimization and user interface design, not the primary focus of cloud governance.

Question 3

Question Type: MultipleChoice

What is the main purpose of Cloud Infrastructure Entitlement Management (CIEM) in cloud environments?

Options:

A- Monitoring network traffic
B- Deploying cloud services
C- Governing access to cloud resources
D- Managing software licensing

Answer:

C

Explanation:

Cloud Infrastructure Entitlement Management (CIEM) is primarily designed togovern access to cloud resources. It addresses the challenges of managing user entitlements and permissions across multi-cloud and hybrid environments. CIEM solutions help organizations manageidentity and access rights, particularly in complex cloud infrastructures where multiple services and user roles are involved.

The primary functions of CIEM include:

Access Governance:Ensuring that the right users have the appropriate level of access to cloud resources.

Least Privilege Enforcement:Automatically identifying and eliminating excessive permissions.

Access Monitoring and Auditing:Continuously tracking permission usage to detect unusual patterns or risks.

Identity Lifecycle Management:Managing the creation, modification, and revocation of identities and their associated permissions.

Why CIEM is Important:

As cloud environments scale, manual management of user roles and permissions becomes unmanageable and prone to errors. CIEM tools automate this process, providingvisibility and control over cloud entitlementsto minimize the risk ofprivilege escalation and unauthorized access.

Why Other Options Are Incorrect:

A . Monitoring network traffic:This falls under network security monitoring and is not related to entitlement management.

B . Deploying cloud services:This involves cloud orchestration and provisioning, not entitlement management.

D . Managing software licensing:CIEM is not concerned with license management, which is handled by software asset management tools.

CSA Security Guidance v4.0, Domain 12: Identity, Entitlement, and Access Management

Cloud Computing Security Risk Assessment (ENISA) - Identity and Access Management

Cloud Controls Matrix (CCM) v3.0.1 - IAM Domain

Question 4

Question Type: MultipleChoice

CCM: Cloud Controls Matrix (CCM) is a completely independent cloud

assessment toolkit that does not map any existing standards.

Options:

A- True
B- False

Answer:

B

Question 5

Question Type: MultipleChoice

Which of the following is a common exploitation factor associated with serverless and container workloads?

Options:

A- Poor Documentation
B- Misconfiguration
C- Insufficient Redundancy
D- Low Availability

Answer:

B

Explanation:

Misconfiguration is one of the most prevalent risks in serverless and container-based environments. Given the complex nature of container orchestration (e.g., Kubernetes), CI/CD pipelines, and ephemeral infrastructure, simple missteps---such as overly permissive roles or exposed ports---can lead to significant vulnerabilities.

These workloads require strict configuration management, automated scanning, and secure defaults to prevent breaches. Unlike traditional servers, containers and functions spin up and down rapidly, making traditional visibility tools insufficient.

This is discussed thoroughly in Domain 8: Virtualization and Containers, where the CCSK guidance identifies misconfiguration as a leading cause of cloud-native exploitation.

CSA Security Guidance v4.0 -- Domain 8: Virtualization and Containers

Question 6

Question Type: MultipleChoice

Which of the following cloud essential characteristics refers to the capability of the service to scale resources up or down quickly and efficiently based on demand?

Options:

A- On-Demand Self-Service
B- Broad Network Access
C- Resource Pooling
D- Rapid Elasticity

Answer:

D

Explanation:

Rapid Elasticity refers to the capability of cloud services to scale resources up or down quickly and efficiently in response to varying demand. This characteristic allows cloud environments to dynamically adjust resource allocation (such as computing power, storage, or bandwidth) to meet the needs of users, ensuring that resources are available when required and minimizing waste when demand decreases.

This ability is a key advantage of cloud computing, providing flexibility and cost efficiency for businesses.

Question 7

Question Type: MultipleChoice

What's the difference between DNS Logs and Flow Logs?

Options:

A- They represent the logging of different networking solutions, and DNS Logs are more suitable for a ZTA implementation
B- DNS Logs record domain name resolution requests and responses, while Flow Logs record info on source, destination, protocol
C- They play identical functions and can be used interchangeably
D- DNS Logs record all the information about the network behavior, including source, destination,

and protocol, while Flow Logs record users' applications behavior

Answer:

B

Explanation:

DNS logs capture information on domain name resolution, while Flow logs capture details about network traffic, including source, destination, and protocol. Reference: [CCSK Study Guide, Domain 7 - Infrastructure & Networking]

P2P exams

Question 8

Question Type: MultipleChoice

What is one main operational challenge associated with using cloud-agnostic container strategies?

Options:

A- Limiting deployment to a single cloud service
B- Establishing identity and access management protocols
C- Reducing the amount of cloud storage used
D- Management plane compatibility and consistent controls

P2P exams

Answer:

D

Explanation:

One of the primary operational challenges associated with using cloud-agnostic container strategies is ensuring management plane compatibility and consistent controls across multiple cloud environments. Cloud-agnostic strategies aim to make containers portable between different cloud providers. However, each cloud provider has its own management tools, APIs, and security controls, which can lead to complexities in maintaining consistent policies, monitoring, and management practices across different cloud environments.

Limiting deployment to a single cloud service is contrary to the goal of a cloud-agnostic strategy,

which seeks to avoid reliance on a single cloud provider. Establishing identity and access management protocols is important but not unique to cloud-agnostic strategies; IAM challenges exist regardless of cloud approach. Reducing the amount of cloud storage used is a general optimization concern, not specifically related to cloud-agnostic containers.

Question 9

Question Type: MultipleChoice

When deploying Security as a Service in a highly regulated industry or environment, what should both parties agree on in advance and include in the SLA?

Options:

A- The metrics defining the service level required to achieve regulatory objectives.
B- The duration of time that a security violation can occur before the client begins assessing regulatory fines.
C- The cost per incident for security breaches of regulated information.
D- The regulations that are pertinent to the contract and how to circumvent them.
E- The type of security software which meets regulations and the number of licenses that will be needed.

Answer:

A

Question 10

Question Type: MultipleChoice

Dynamic Application Security Testing (DAST) might be limited or require pre-testing permission from the provider.

Options:

A- False
B- True

Answer:

B

Question 11

Question Type: MultipleChoice

Which of the following is true about access policies in cybersecurity?

Options:

A- They are used to monitor real-time network traffic
B- They are solely concerned with user authentication methods
C- They provide data encryption protocols for secure communication
D- They define permissions and network rules for resource access

Answer:

D

Explanation:

Access policies in cybersecurity are critical for managing and controlling how users and devices access resources within a network or cloud environment. These policies are primarily concerned with defining permissions and rules that govern access to resources. They help organizations implement role-based access control (RBAC) or attribute-based access control (ABAC), which specify who can access what resources and under what conditions.

In the context of cloud computing, access policies are typically enforced using Identity and Access Management (IAM) tools and services, which allow administrators to define and manage the permissions associated with user identities. Access policies include various rules that specify allowed or denied actions based on roles, user attributes, device types, or network conditions.

For example, in the AWS environment, access policies are written in JSON and define permissions for services like EC2, S3, or RDS. Similarly, Azure uses Role-Based Access Control (RBAC) to manage resource access policies.

Access policies are not concerned with real-time monitoring (option A), user authentication methods (option B), or encryption protocols (option C). Instead, they explicitly focus on defining access permissions and controlling how resources are utilized.

CSA Security Guidance v4.0, Domain 12: Identity, Entitlement, and Access Management

Cloud Computing Security Risk Assessment (ENISA) - Identity and Access Management section

Cloud Controls Matrix (CCM) v3.0.1 - IAM Domain

To Get Premium Files for CCSK Visit
https://www.p2pexams.com/products/ccsk

For More Free Questions Visit
https://www.p2pexams.com/csa/pdf/ccsk