



CSA CCSK Practice Questions

Shared by Downs on 08-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

If in certain litigations and investigations, the actual cloud application or environment itself is relevant to resolving the dispute in the litigation or investigation, how is the information likely to be obtained?

Options:

- A- It may require a subpoena of the provider directly
- B- It would require a previous access agreement
- C- It would require an act of war
- D- It would require a previous contractual agreement to obtain the application or access to the environment
- E- It would never be obtained in this situation

Answer:

D

Question 2

Question Type: MultipleChoice

Which approach is commonly used by organizations to manage identities in the cloud due to the complexity of scaling across providers?

Options:

- A- Decentralization
- B- Centralization
- C- Federation
- D- Outsourcing

Answer:

C

Explanation:

Managing identities across multiple cloud providers is complex due to the need for scalability, interoperability, and consistent access control. The federation approach is commonly used to address this challenge. Identity federation allows organizations to use a single set of credentials across different cloud providers by leveraging standards such as SAML, OAuth, or OpenID Connect. This enables seamless authentication and authorization without requiring separate identity management systems for each provider.

From the CCSK v5.0 Study Guide, Domain 6 (Identity, Entitlement, and Access Management), Section 6.3:

"Identity federation is a critical approach for managing identities in cloud environments, especially when scaling across multiple providers. Federation allows organizations to use a trusted identity provider (IdP) to authenticate users, enabling single sign-on (SSO) and consistent access control across disparate cloud services."

Option C (Federation) is the correct answer.

Option A (Decentralization) is incorrect because decentralizing identity management increases complexity and reduces consistency across providers.

Option B (Centralization) is incorrect because, while centralized identity management may be used within a single organization, it does not scale effectively across multiple cloud providers without federation.

Option D (Outsourcing) is incorrect because outsourcing identity management does not inherently address the scalability and interoperability challenges of cloud environments.

CCSK v5.0 Study Guide, Domain 6, Section 6.3: Identity Federation.

CSA Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, Domain 11.

Question 3

Question Type: MultipleChoice

Which option best describes the advantage of custom application level encryption?

Options:

- A- It simplifies the encryption process by centralizing it at the network level
- B- It enables ownership and more granular control of encryption keys
- C- It reduces the need for encryption by enhancing network security
- D- It delegates the control of keys to third-party providers

Answer:

B

Explanation:

Custom application-level encryption provides organizations with precise control over what is encrypted and who manages the encryption keys. Unlike network-level encryption, this method allows sensitive fields (e.g., credit card numbers) to be encrypted before data even enters the storage or processing pipeline.

This approach enables compliance with strict data privacy laws and protects data from being decrypted by unauthorized actors—even cloud providers. Organizations can enforce key rotation policies and maintain exclusive key access.

This is detailed in Domain 11: Data Security and Encryption, which recommends application-level encryption for sensitive data protection, particularly in regulated industries.

CSA Security Guidance v4.0 -- Domain 11: Data Security and Encryption

=====

Question 4

Question Type: MultipleChoice

In the context of cloud security, which approach prioritizes incoming data logs for threat detection by applying multiple sequential filters?

Options:

- A- Cascade-and-filter approach
- B- Parallel processing approach
- C- Streamlined single-filter method
- D- Unfiltered bulk analysis

Answer:

A

Explanation:

The Cascade-and-filter approach is a method used in cloud security to handle incoming data logs efficiently. It prioritizes logs for threat detection by applying multiple sequential filters, where each filter progressively narrows down the data. This approach helps in:

Layered threat detection: Early filters eliminate non-critical data, while subsequent filters perform more detailed analysis.

Efficient processing: Reduces the volume of data passed through advanced and resource-intensive filters.

Improved accuracy: Allows focusing on the most relevant security events.

For example, in a cloud environment, the first filter might check for known malicious IP addresses, the second might look for suspicious file types, and subsequent filters may perform behavioral analysis or anomaly detection.

Why Other Options Are Incorrect:

B . Parallel processing approach: This method processes logs simultaneously, not sequentially, and is less efficient for prioritizing threats.

C . Streamlined single-filter method: Uses a single filter for all data, which lacks depth and thoroughness in identifying complex threats.

D . Unfiltered bulk analysis: This approach is resource-intensive and inefficient, as it does not prioritize or filter logs.

CSA Security Guidance v4.0, Domain 9: Incident Response

Cloud Computing Security Risk Assessment (ENISA) - Log Management and Threat Detection

Cloud Controls Matrix (CCM) v3.0.1 - Logging and Monitoring Domain

Question 5

Question Type: MultipleChoice

Which of the following events should be monitored according to CIS AWS benchmarks?

Options:

- A- Regular file backups
- B- Data encryption at rest
- C- Successful login attempts
- D- Unauthorized API calls

Answer:

D

Explanation:

According to the CIS AWS (Center for Internet Security AWS) benchmarks, unauthorized API calls should be closely monitored because they indicate potential security threats or malicious activity within the AWS environment. Monitoring unauthorized API calls helps detect unauthorized access, misconfigurations, or attempts to exploit cloud resources. It's a key part of maintaining a secure AWS environment and helps ensure compliance with security best practices.

Regular file backups are important but not specifically a focus of the CIS AWS benchmarks. Data encryption at rest is a security best practice but monitoring unauthorized API calls directly addresses access control and security within the environment. Successful login attempts are important but monitoring failed login attempts (as opposed to successful ones) is generally a better practice for identifying suspicious activity.

Question 6

Question Type: MultipleChoice

What does orchestration automate within a cloud environment?

Options:

- A- Monitoring application performance
- B- Manual configuration of security policies
- C- Installation of operating systems
- D- Provisioning of VMs, networking and other resources

Answer:

D

Explanation:

In a cloud environment, orchestration automates the provisioning and management of various cloud resources, including virtual machines (VMs), networking, storage, and other infrastructure components. Cloud orchestration involves the use of software to coordinate and

automate tasks that would otherwise require manual intervention, improving efficiency, scalability, and consistency across the environment.

Monitoring application performance is typically handled by monitoring tools, not orchestration. Manual configuration of security policies is something that can be automated through policy management but is not the focus of orchestration. Installation of operating systems is part of provisioning resources, but orchestration primarily focuses on automating the overall management of infrastructure and services, not just the installation of operating systems.

Question 7

Question Type: MultipleChoice

Which data security control is the LEAST likely to be assigned to an IaaS provider?

Options:

- A- Application logic
- B- Access controls
- C- Encryption solutions
- D- Physical destruction
- E- Asset management and tracking

Answer:

A

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>

20%
DISCOUNT

P2P
exams