Free Questions for CCSK

Shared by Sandoval on 13-05-2025

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is a key benefit of using customer-managed encryption keys with cloud key management service (KMS)?

Options:

A- Customers can bypass the need for encryption
B- Customers retain control over their encryption keys
C- Customers can share their encryption keys more easily
D- It reduces the computational load on the cloud service provider

Answer:

B

Explanation:

The correct answer is B. Customers retain control over their encryption keys.

Using customer-managed encryption keys (CMEK) with a cloud Key Management Service (KMS) allows the customer to retain full control over the encryption keys used to encrypt their data. This is crucial in maintaining data sovereignty, privacy, and compliance with regulatory requirements.

Key Benefits of Customer-Managed Encryption Keys:

Key Ownership and Control: Unlike cloud provider-managed keys, CMEK ensures that the customer has full authority over the key's lifecycle, including creation, rotation, and deletion.

Enhanced Security: Customers can enforce strict access controls and audit who accesses the keys.

Compliance: Many regulations (like GDPR or HIPAA) mandate that data owners maintain control over encryption keys.

Data Privacy: Even though the data is stored on the cloud, the provider cannot access unencrypted data without the customer's permission.

Flexibility: Customers can choose when to revoke or rotate keys, which directly impacts data availability and access.

Why Other Options Are Incorrect:

A . Bypass the need for encryption: CMEK does not eliminate the need for encryption; it

strengthens it by giving customers direct control.

C . Share encryption keys more easily: Sharing encryption keys can increase security risks, and CMEK is designed to restrict, not ease, key sharing.

D . Reduces computational load on the cloud service provider: CMEK does not impact the computational load. It focuses on key management and control rather than reducing processing overhead.

Real-World Example:

In AWS KMS, using CMEK allows customers to bring their own keys (BYOK) and manage them directly through AWS Key Management Service. Similar practices exist in Google Cloud KMS and Azure Key Vault, where customers can generate and control their own encryption keys.

Practical Use Case:

A healthcare provider using a cloud service to store patient records may use CMEK to ensure that sensitive data is encrypted under keys they control, ensuring compliance with regulations like HIPAA.

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

Cloud Computing Security Risk Assessment (ENISA) - Key Management and Encryption

Cloud Controls Matrix (CCM) v3.0.1 - Data Protection and Encryption Domain

Question 2

Question Type: MultipleChoice

Which of the following is a primary benefit of using Infrastructure as Code (IaC) in a security context?

Options:

A- Manual patch management
B- Ad hoc security policies
C- Static resource allocation
D- Automated compliance checks

Answer:

D

Explanation:

The correct answer is D. Automated compliance checks.

Infrastructure as Code (IaC) is a key DevSecOps practice where infrastructure configurations are defined and managed through code. In a security context, the primary benefit of using IaC is the ability to automate compliance checks and enforce security best practices consistently across environments.

Key Benefits of IaC in Security:

Automated Compliance: IaC allows for the embedding of security policies directly into configuration scripts. This means that when infrastructure is deployed, it automatically adheres to compliance requirements (like NIST, CIS benchmarks).

Consistency and Repeatability: Since IaC scripts are version-controlled, any configuration changes are tracked, minimizing the risk of configuration drift.

Security by Design: By coding security configurations (like IAM roles, network ACLs, encryption settings), organizations ensure that every deployment meets security standards.

Reduced Human Error: Automating infrastructure provisioning reduces manual errors that can lead to vulnerabilities.

Why Other Options Are Incorrect:

A . Manual patch management: IaC promotes automated and repeatable configurations, reducing the need for manual patching.

B . Ad hoc security policies: IaC encourages standardized and consistent policies rather than ad hoc management.

C . Static resource allocation: IaC is dynamic and scalable, allowing for automatic scaling and configuration management rather than static resource setups.

Real-World Example:

Using tools like Terraform or AWS CloudFormation, organizations can define IAM policies, security group rules, and data encryption settings as part of the infrastructure code. These configurations are then automatically checked for compliance against established policies during deployment.

Security and Compliance in IaC:

Organizations can integrate tools like Terraform Compliance or AWS Config Rules to automatically verify that infrastructure settings align with regulatory requirements and internal security policies.

CSA Security Guidance v4.0, Domain 10: Application Security

Cloud Computing Security Risk Assessment (ENISA) - Infrastructure as Code Best Practices

Cloud Controls Matrix (CCM) v3.0.1 - Configuration and Change Management Domain

Question 3

Question Type: MultipleChoice

In the context of Software-Defined Networking (SDN), what does decoupling the network control plane from the data plane primarily achieve?

Options:

A- Enables programmatic configuration
B- Decreases network security
C- Increases hardware dependency
D- Increases network complexity

Answer:

A

Explanation:

The correct answer is A. Enables programmatic configuration.

In Software-Defined Networking (SDN), the control plane and data plane are decoupled, meaning that the network intelligence (control plane) is separated from the traffic forwarding functions (data plane). This separation allows network control to be directly programmable, rather than embedded within the hardware.

Key Benefits of Decoupling:

Programmatic Configuration: Network administrators can program the network dynamically using software applications. This programmability enables automated, flexible, and efficient network management.

Centralized Control: The control plane is managed from a centralized controller, which can adjust network configurations in real-time.

Reduced Hardware Dependency: Since the control logic is no longer embedded in individual hardware devices, it is easier to use commodity hardware and standardized interfaces.

Agility and Scalability: Organizations can rapidly deploy new services and update configurations

without altering the underlying hardware.

Why Other Options Are Incorrect:

B . Decreases network security: Decoupling does not inherently decrease security. In fact, centralized control can enhance security through consistent policy enforcement.

C . Increases hardware dependency: The opposite is true. SDN reduces dependency on proprietary hardware by enabling software-based management.

D . Increases network complexity: While SDN introduces new software components, it simplifies network management by centralizing control and reducing hardware configuration complexities.

Real-World Example:

In a cloud environment, SDN controllers like OpenDaylight or Cisco ACI allow for dynamic routing, load balancing, and traffic management through APIs. This flexibility supports automated scaling and traffic optimization.

CSA Security Guidance v4.0, Domain 7: Infrastructure Security

Cloud Computing Security Risk Assessment (ENISA) - SDN and Network Virtualization

Cloud Controls Matrix (CCM) v3.0.1 - Network Security Domain

Question 4

Question Type: MultipleChoice

Which tool is most effective for ensuring compliance and identifying misconfigurations in cloud management planes?

Options:

A- Data Security Posture Management (DSPM)
B- SaaS Security Posture Management (SSPM)
C- Cloud Detection and Response (CDR)
D- Cloud Security Posture Management (CSPM)

Answer:

D

Explanation:

The correct answer is D. Cloud Security Posture Management (CSPM).

Cloud Security Posture Management (CSPM) is a comprehensive tool designed to identify and remediate misconfigurations and compliance violations in cloud management planes. It helps organizations maintain secure and compliant cloud environments by continuously monitoring configurations against industry standards and best practices.

Key Functions of CSPM:

Configuration Management: Identifies misconfigurations and alerts administrators to fix them.

Compliance Monitoring: Continuously assesses cloud environments against compliance frameworks such as CIS, NIST, GDPR, and others.

Automated Remediation: Automatically fixes known configuration errors based on predefined policies.

Visibility: Provides a comprehensive view of security and compliance risks across multi-cloud environments.

Risk Assessment: Analyzes risks related to identity, data exposure, and network configurations.

Why CSPM is Most Effective:

Cloud environments are dynamic, and maintaining secure configurations is challenging. CSPM solutions like AWS Config, Azure Security Center, and Google Cloud Security Command Center automate the process of checking for security policy violations and configuration drift.

Why Other Options Are Incorrect:

A . Data Security Posture Management (DSPM): Focuses on data security, data loss prevention, and data governance, rather than configuration and compliance management.

B . SaaS Security Posture Management (SSPM): Specifically targets SaaS applications, managing security settings and compliance of cloud-based software rather than infrastructure.

C . Cloud Detection and Response (CDR): Focuses on threat detection and incident response rather than configuration management and compliance.

Real-World Example:

A CSPM tool like Palo Alto Prisma Cloud or AWS Config can automatically detect if IAM policies are overly permissive or if S3 buckets are publicly accessible, helping to maintain compliance and reduce attack surfaces.

CSA Security Guidance v4.0, Domain 4: Compliance and Audit Management

Cloud Computing Security Risk Assessment (ENISA) - Cloud Security Monitoring

Cloud Controls Matrix (CCM) v3.0.1 - Cloud Configuration Management Domain

Question 5

Question Type: MultipleChoice

What is the primary function of a Load Balancer Service in a Software Defined Network (SDN) environment?

Options:

A- To create isolated virtual networks
B- To monitor network performance and activity
C- To distribute incoming network traffic across multiple destinations
D- To encrypt data for secure transmission

Answer:

C

Explanation:

The correct answer is C. To distribute incoming network traffic across multiple destinations.

A Load Balancer Service in an SDN environment is responsible for efficiently distributing network traffic across multiple servers or instances. This ensures high availability, reliability, and optimized resource usage.

Key Functions:

Traffic Distribution: Balances incoming requests to various servers based on predefined algorithms (round-robin, least connections, etc.).

High Availability: Prevents server overload and reduces downtime by distributing workload.

Scalability: Automatically adjusts as the number of requests or available resources changes.

Health Monitoring: Continually checks server availability and responsiveness to avoid directing traffic to non-responsive instances.

Why Other Options Are Incorrect:

A . Isolated virtual networks: Creating isolated networks is a function of network virtualization, not load balancing.

B . Monitor network performance: Monitoring is done by network monitoring tools, not load balancers.

D . Encrypt data for secure transmission: Encryption is handled by security protocols like TLS/SSL, not load balancers.

Real-World Example:

Services like AWS Elastic Load Balancer (ELB) and Azure Load Balancer ensure that traffic is distributed efficiently across instances, maintaining performance and uptime.

CSA Security Guidance v4.0, Domain 7: Infrastructure Security

Cloud Computing Security Risk Assessment (ENISA) - SDN and Load Balancing

Cloud Controls Matrix (CCM) v3.0.1 - Network and Infrastructure Domains

Question 6

Question Type: MultipleChoice

Which aspects are most important for ensuring security in a hybrid cloud environment?

Options:

A- Use of encryption for all data at rest
B- Implementation of robust IAM and network security practices
C- Regular software updates and patch management
D- Deployment of multi-factor authentication only

Answer:

B

Explanation:

The correct answer is B. Implementation of robust IAM and network security practices.

A hybrid cloud environment involves integrating private and public cloud infrastructures. This setup requires enhanced security practices to manage the complexity and diverse security requirements of both environments.

Key Aspects:

Identity and Access Management (IAM): Ensures secure authentication and authorization across both private and public clouds.

Network Security: Includes securing data in transit, implementing network segmentation, and protecting communication between cloud environments.

Unified Security Policies: Establishing consistent policies and access controls across both environments.

Visibility and Monitoring: Continuous monitoring of network traffic and access logs to detect potential threats.

Why Other Options Are Incorrect:

A . Encryption for data at rest: Important but not the most comprehensive security measure for hybrid environments.

C . Software updates and patch management: While essential, these practices alone do not address the complex challenges of a hybrid setup.

D . Multi-factor authentication only: MFA enhances authentication security but does not cover the broader security requirements of a hybrid cloud.

Real-World Context:

Organizations using services like AWS Direct Connect or Azure ExpressRoute to integrate on-premises environments with the public cloud must implement robust IAM and network security practices to maintain secure and compliant data flows.

CSA Security Guidance v4.0, Domain 7: Infrastructure Security

Cloud Computing Security Risk Assessment (ENISA) - Hybrid Cloud Security

Cloud Controls Matrix (CCM) v3.0.1 - Network and IAM Domains

==========

Question 7

Question Type: MultipleChoice

Which of the following best describes the concept of Measured Service in cloud computing?

Options:

A- Cloud systems allocate a fixed immutable set of measured services to each customer.

B- Cloud systems offer elastic resources.
C- Cloud systems provide usage reports upon request, based on manual reporting.
D- Cloud systems automatically monitor resource usage and provide billing based on actual consumption.

Answer:

D

Explanation:

The correct answer is D. Cloud systems automatically monitor resource usage and provide billing based on actual consumption.

Measured Service is one of the essential characteristics of cloud computing as defined by the NIST (National Institute of Standards and Technology). It implies that cloud systems automatically control and optimize resource usage by leveraging a metering capability. This capability tracks and reports resource consumption (such as CPU, storage, or bandwidth), which is used for billing, monitoring, and planning.

Key Characteristics:

Automatic Monitoring: Cloud platforms continuously track resource usage without manual intervention.

Billing Based on Usage: Customers are billed based on the actual consumption of resources (pay-as-you-go model).

Transparency: Users can view detailed usage reports to understand their resource utilization and associated costs.

Resource Optimization: Providers use these metrics to optimize resource allocation and improve efficiency.

Why Other Options Are Incorrect:

A . Fixed immutable set of measured services: This contradicts the concept of elasticity and resource pooling in cloud computing.

B . Elastic resources: While elasticity is a cloud characteristic, it does not directly define measured service.

C . Manual reporting: Measured service is about automated, real-time monitoring and billing, not manual data gathering.

Real-World Example:

In AWS, services like Amazon CloudWatch automatically collect and provide usage metrics, and

the AWS Billing Console shows the cost associated with each resource.

CSA Security Guidance v4.0, Domain 1: Cloud Computing Concepts and Architectures

NIST SP 800-145 - The NIST Definition of Cloud Computing

Cloud Controls Matrix (CCM) v3.0.1 - Metering and Billing Domain

==========

Question 8

Question Type: MultipleChoice

What Identity and Access Management (IAM) process decides to permit or deny a subject access to system objects like networks, data, or applications?

Options:

A- Authorization
B- Federation
C- Authentication
D- Provisioning

Answer:

A

Explanation:

The correct answer is A. Authorization. In Identity and Access Management (IAM), authorization is the process of determining whether a subject (user, application, or device) has the right to access a specific system object, such as networks, data, or applications. Authorization decisions are made after successful authentication and are based on the subject's permissions, roles, or attributes.

Key Characteristics of Authorization:

Decision Making: Determines if access is permitted or denied based on policies or permissions.

Role and Attribute-Based Access: Often uses Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC) mechanisms to enforce policies.

Post-Authentication Process: Occurs after authentication has verified the user's identity.

Resource-Specific: Determines the level of access or specific operations (like read, write, execute) a user is allowed.

Example Scenario:

When a user logs into a cloud platform, the system first authenticates the user (verifies their identity) and then authorizes their access to specific resources, such as viewing data in an S3 bucket or managing a VM instance. The access policies define what actions the authenticated user can perform.

Why Other Options Are Incorrect:

B . Federation: Involves linking a user's identity across multiple systems or domains but does not decide access permissions.

C . Authentication: The process of verifying a user's identity, typically through passwords, biometrics, or multi-factor authentication (MFA), but it does not determine resource access.

D . Provisioning: Refers to creating and managing user accounts and permissions, but it does not make real-time access decisions.

Real-World Context:

In cloud environments, services like AWS IAM or Azure AD use policies to authorize user actions after they have been authenticated. For instance, an AWS IAM policy might allow a user to list S3 buckets but deny deletion.

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

Cloud Computing Security Risk Assessment (ENISA) - IAM and Access Control

Cloud Controls Matrix (CCM) v3.0.1 - Identity and Access Management Domain

Question 9

Question Type: MultipleChoice

A company plans to shift its data processing tasks to the cloud. Which type of cloud workload best describes the use of software emulations of physical computers?

Options:

A- Platform as a Service (PaaS)

B- Serverless Functions (FaaS)
C- Containers
D- Virtual Machines (VMs)

Answer:

D

Explanation:

The correct answer is D. Virtual Machines (VMs). In the context of cloud computing, Virtual Machines (VMs) are software-based emulations of physical computers. They run an operating system (OS) and applications just like a physical machine would. VMs are often hosted on physical servers using hypervisors, which allow multiple VMs to run on a single physical machine, thereby sharing resources like CPU, memory, and storage.

Why Virtual Machines (VMs) are Suitable for Data Processing:

Full OS Environment: VMs provide a complete operating system environment, making them suitable for running complex data processing tasks that require specific OS configurations.

Isolation: Each VM operates independently, providing isolation between different workloads, which is essential when processing sensitive or diverse data sets.

Scalability: Cloud providers offer VM scaling options to meet the demands of data processing workloads.

Compatibility: VMs can run legacy applications that may not be compatible with newer cloud-native technologies.

Why Other Options Are Incorrect:

A . Platform as a Service (PaaS): PaaS provides a platform for developing and deploying applications without managing underlying infrastructure. It is not directly related to VM-based processing.

B . Serverless Functions (FaaS): Serverless computing abstracts the infrastructure and is used for running discrete functions rather than emulating entire machines.

C . Containers: Containers package applications and dependencies but share the host OS kernel. They are lightweight compared to VMs and do not fully emulate physical computers.

Real-World Example:

If a company moves a data processing application that was traditionally run on an on-premises physical server to the cloud, they might choose VMs on services like AWS EC2, Azure Virtual Machines, or Google Compute Engine to maintain the same OS environment and application compatibility.

CSA Security Guidance v4.0, Domain 7: Infrastructure Security

Cloud Computing Security Risk Assessment (ENISA) - Virtualization Risks

Cloud Controls Matrix (CCM) v3.0.1 - Infrastructure as a Service (IaaS) Domain

Question 10

Question Type: MultipleChoice

What is the primary 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 to govern access to cloud resources. It addresses the challenges of managing user entitlements and permissions across multi-cloud and hybrid environments. CIEM solutions help organizations manage identity 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, providing visibility and control over cloud entitlements to minimize the risk of privilege 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

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

