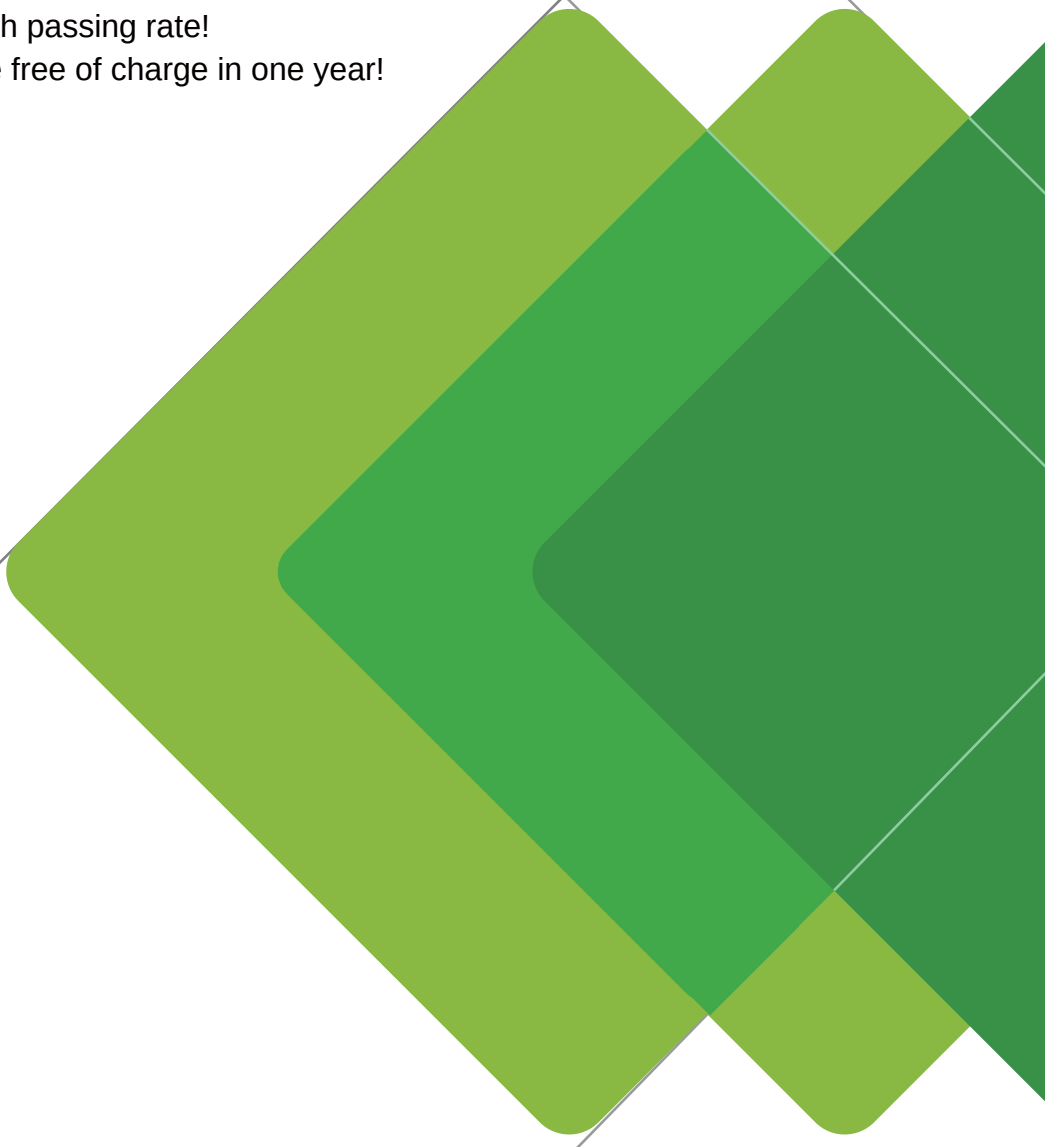
IT-DUMPS Q&A

Accurate study guides, High passing rate!
IT-dumps provides update free of charge in one year!



Exam : **CCSK**

Title : Certificate of Cloud Security Knowledge

Version : DEMO

1.Which of the following best describes the responsibility for security in a cloud environment?
A. Cloud Service Customers (CSCs) are solely responsible for security in the cloud environment. The Cloud Service Providers (CSPs) are accountable.
B. Cloud Service Providers (CSPs) and Cloud Service Customers (CSCs) share security responsibilities. The exact allocation of responsibilities depends on the technology and context.
C. Cloud Service Providers (CSPs) are solely responsible for security in the cloud environment. Cloud Service Customers (CSCs) have an advisory role.
D. Cloud Service Providers (CSPs) and Cloud Service Customers (CSCs) share security responsibilities. The allocation of responsibilities is constant.
Answer: B
Explanation:
The shared security responsibility model in cloud environments clarifies that CSPs and CSCs both have roles, with specific responsibilities varying based on the service model (IaaS, PaaS, SaaS). In IaaS, CSCs handle more security, while CSPs manage most security in SaaS.
Reference: [CCSK Study Guide, Domain 1 - Cloud Security Scope and Responsibilities] [16†source].

2.In the Incident Response Lifecycle, which phase involves identifying potential security events and examining them for validity?
A. Post-Incident Activity
B. Detection and Analysis
C. Preparation
D. Containment, Eradication, and Recovery
Answer: B
Explanation:
The Detection and Analysis phase involves identifying incidents and determining their impact. It is crucial to validate events to understand if they constitute a security incident.
Reference: [Security Guidance v5, Domain 11 - Incident Response]

3.How does centralized logging simplify security monitoring and compliance?
A. It consolidates logs into a single location.
B. It decreases the amount of data that needs to be reviewed.
C. It encrypts all logs to prevent unauthorized access.
D. It automatically resolves all detected security threats.
Answer: A
Explanation:
Centralized logging aggregates logs in one location, making it easier to monitor, analyze, and comply with regulatory requirements.
Reference: [Security Guidance v5, Domain 6 - Security Monitoring]

4.Why is early integration of pre-deployment testing crucial in a cybersecurity project?
A. It identifies issues before full deployment, saving time and resources.
B. It increases the overall testing time and costs.
C. It allows skipping final verification tests.
D. It eliminates the need for continuous integration.

Answer: A
Explanation:
Integrating testing early helps identify security vulnerabilities and configuration issues before they reach production, reducing remediation costs and time.
Reference: [Security Guidance v5, Domain 10 - Application Security]

5.What process involves an independent examination of records, operations, processes, and controls within an organization to ensure compliance with cybersecurity policies, standards, and regulations?
A. Risk assessment
B. Audit
C. Penetration testing
D. Incident response
Answer: B
Explanation:
Auditing is an independent review process that validates adherence to policies, regulations, and standards. It is essential in assessing security posture.
Reference: [Security Guidance v5, Domain 3 - Compliance] [16†source].