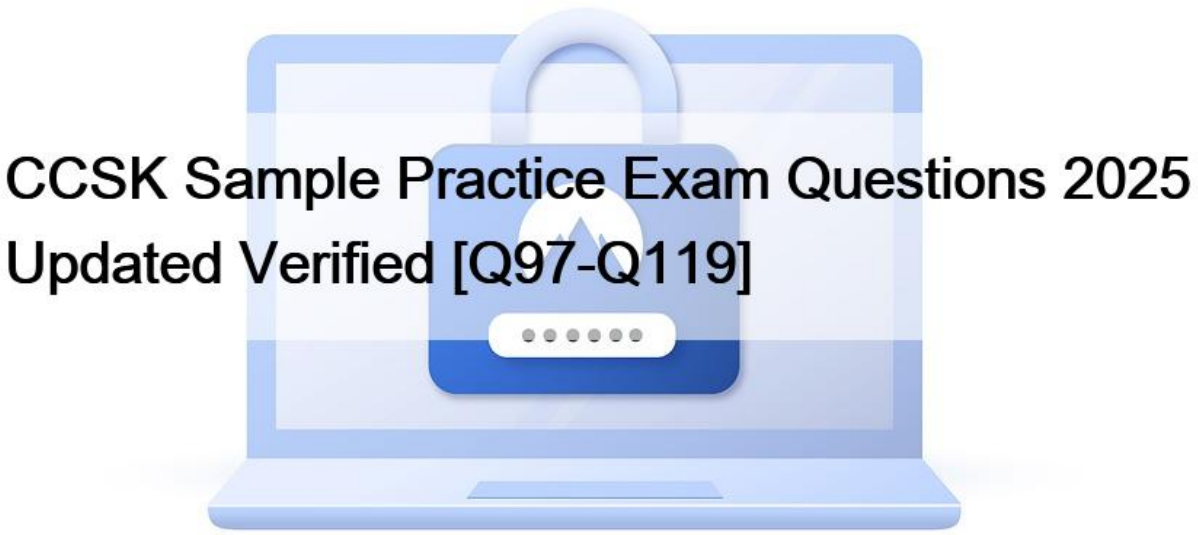
CCSK Sample Practice Exam Questions 2025 Updated Verified [Q97-Q119



CCSK Sample Practice Exam Questions 2025 Updated Verified Exam Study Guide Free Practice Test LAST UPDATED

CCSK NEW QUESTION 97

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?

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

NEW QUESTION 98

Which cloud storage technology is basically a virtual hard drive for instanced or VMs?

* Volume storage
* Platform
* Database
* Application
* Object storage

NEW QUESTION 99

What factors should you understand about the data specifically due to legal, regulatory, and jurisdictional factors?

* The physical location of the data and how it is accessed
* The fragmentation and encryption algorithms employed
* The language of the data and how it affects the user
* The implications of storing complex information on simple storage systems
* The actual size of the data and the storage format

NEW QUESTION 100

What is a core tenant of risk management?
* The provider is accountable for all risk management.
* You can manage, transfer, accept, or avoid risks.
* The consumers are completely responsible for all risk.
* If there is still residual risk after assessments and controls are in

place, you must accept the risk.
* Risk insurance covers all financial losses, including loss of customers.

NEW QUESTION 101

Which of the following Storage type is NOT associated with SaaS solution?
* Content Delivery network
* Raw Storage
* Volume Storage
* Ephemeral Storage

Volume storage is commonly associated with IaaS solutions.

All the other 3 options are related to SaaS solutions

NEW QUESTION 102

In the shared security model, how does the allocation of responsibility vary by service?
* Shared responsibilities should be consistent across all services.
* Based on the per-service SLAs for security.
* Responsibilities are the same across IaaS, PaaS, and SaaS in the shared model.
* Responsibilities are divided between the cloud provider and the customer based on the service type.

The division of security responsibilities changes according to the service model. In IaaS, CSCs handle more security responsibilities, while in SaaS, the CSP manages more of the security aspects. Reference: [Security Guidance v5, Domain 1 – Shared Responsibility Model]

NEW QUESTION 103

Which is the key technology that enables the sharing of resources and makes cloud computing most viable in terms of cost savings?
* Scalability
* Virtualization
* Software Defined Networking(SDN)
* Content Delivery Networks(CDN)

Virtualization is the foundational technology that underlies and makes cloud computing possible.

Virtualization is based on the use of powerful host computers to provide a shared resource pool that can be managed to maximize the number of guest operating systems(OSs) running on each host.

NEW QUESTION 104

Which areas should be initially prioritized for hybrid cloud security?
* Cloud storage management and governance
* Data center infrastructure and architecture
* IAM and networking
* Application development and deployment

Identity and Access Management (IAM) and networking are essential for secure hybrid cloud environments, as they control access and communication across diverse environments. Reference: [Security Guidance v5, Domain 5 – IAM]

NEW QUESTION 105

Cloud architectures necessitate certain roles which are extremely high-risk. Examples of such roles include CP system administrators and auditors and managed security service providers dealing with intrusion detection reports and incident response. They are known as high-risk because their malicious activities can lead to abuse of high privilege roles and can impact confidentiality, integrity and availability of data.
* True
* False

NEW QUESTION 106

Multi-tenancy and shared resources are defining characteristics of cloud computing. However, mechanisms separating storage, memory, routing may fail due to several reasons. What risk are we talking about?
* Isolation Failure
* Isolation Escalation
* Separation of Duties
* Route poisoning

According to ENISA (European Network and Information Security Agency) document on Security risk and recommendation, Isolation failure is considered as one of the top risk and is defined as follows Multi- tenancy and shared resources are defining characteristics of cloud computing. This risk category covers the failure of mechanisms separating storage, memory, routing and even reputation between different tenants (e.g, so-called guest-hopping attacks). However it should be considered that attacks on resource isolation mechanisms (e.g. against hypervisors) are still less numerous and much more difficult for an attacker to put in practice compared to attacks on traditional Oss.

NEW QUESTION 107

Which of the following encryption methods would be utilized when object storage is used as the back-end for an application?
* Database encryption
* Media encryption
* Asymmetric encryption
* Object encryption
* Client/application encryption

NEW QUESTION 108

Which is the most common control used for Risk Transfer?
* Contracts
* SLA
* Insurance

* Web Application Firewall

Buying insurance is most common method of transferring risk.

NEW QUESTION 109

Exploitable bugs in programs that attackers can use to infiltrate a computer system for the purpose of stealing data, taking control of the system or disrupting service operations, are called:

* Threat Agents
* Honepots
* Threats
* Vulnerbilities

NEW QUESTION 110

No policy on resource capping can lead to:

* Data disclosure
* Data manipulation
* Resource manipulation
* Resource Exhaustion

It can lead to resource exhaustion if you do not put upper limit on resource allocation.

Cloud services are on-demand Therefore there is a level of calculated risk in allocating all the resources of a cloud service, because resources are allocated according to statistical projections. In accurate modelling of resources usage- common resources allocation algorithms are vulnerable to distortions of fairness

NEW QUESTION 111

Why is a service type of network typically isolated on different hardware?

* It requires distinct access controls
* It manages resource pools for cloud consumers
* It has distinct functions from other networks
* It manages the traffic between other networks
* It requires unique security

NEW QUESTION 112

Lack of CPU or network bandwidth and intermittent access to provisioned resources are examples of which of the following cloud risk?

* Isolation failure
* Software vulnerabilities
* API vulnerabilities
* Resource Exhaustion

They are all examples of resource exhaustion

NEW QUESTION 113

What is the key benefit provided to the customer in Infrastructure as a Service model?

* Transfer of cost of ownership
* Scalability
* Governance

* Reduction of Risk

Transfer of cost of ownership is the key benefit of IaaS model.

NEW QUESTION 114

The intermediary that provides connectivity and transport of cloud services between the CSPs and the cloud service consumers is called:

* Cloud Service Broker
* Cloud Access Service Broker
* Cloud Reseller
* Cloud Carrier

All the terms given as options are very important and candidate is expected to know them and differentiate between them

NEW QUESTION 115

What is a key consideration when implementing AI workloads to ensure they adhere to security best practices?

* AI workloads do not require special security considerations compared to other workloads.
* AI workloads should be openly accessible to foster collaboration and innovation.
* AI workloads should be isolated in secure environments with strict access controls.
* Security practices for AI workloads should focus solely on protecting the AI models.

AI workloads often require isolation and strict access controls to prevent unauthorized access and safeguard sensitive data involved in machine learning processes. Reference: [CCSK Study Guide, Domain 8 – AI Workload Security]

NEW QUESTION 116

NIST defines five characteristics of cloud computing- Rapid Elasticity, Broad Network Access, 0n demand self-service, Metered Usage & Resource pooling. However, IS0/lEC17788 mentions one more characteristic in addition is those 5. Which of the following is that characterstic?

* Multitenancy
* Isolation
* Segregation
* Automation

IS0/lEC17788 lists six key characteristics. the first five of which are identical to the NIST characteristics.

The only addition is multitenancy. which is distinct from resource pooling.

Ref: CSA Security Guidelines V4.0

NEW QUESTION 117

In the Incident Response Lifecycle, which phase involves identifying potential security events and examining them for validity?

* Post-Incident Activity
* Detection and Analysis
* Preparation
* Containment, Eradication, and Recovery

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]

NEW QUESTION 118

Which of the following is a perceived advantage or disadvantage of managing enterprise risk for cloud deployments?
* More physical control over assets and processes.
* Greater reliance on contracts, audits, and assessments due to lack of visibility or management.
* Decreased requirement for proactive management of relationship and adherence to contracts.
* Increased need, but reduction in costs, for managing risks accepted by the cloud provider.
* None of the above.

Explanation/Reference:

NEW QUESTION 119

In the IaaS hosted environment. who is ultimately responsible for platform security?
* Joint responsibility
* Cloud Service Provider
* System Administrator
* Customer

In IaaS hosted environment, Platform security is responsibility of the customer whereas infrastructure security is a shared responsibility between cloud service provider and the customer

The benefit of obtaining the Certificate of Cloud Security Knowledge (CCSK) Exam Certification

By earning this certification, candidates will enjoy the following benefits:

- In dealing with a wide range of responsibilities, from cloud governance to configuring technical security controls, learn to create a baseline of security best practices- Other credentials such as CISA, CISSP, and CCSP are complemented- Increase job prospects for cloud-certified professionals by filling the skills gap- Display their technological expertise, experience, and abilities to use controls adapted to the cloud effectively- Prove their experience with a company that specializes in cloud research on key cloud security issues

Cloud Security Alliance CCSK (Certificate of Cloud Security Knowledge) Certification Exam is a globally recognized certification program that validates an individual's knowledge of cloud security principles, concepts, and best practices. Developed by the Cloud Security Alliance, the exam is designed to assess an individual's competence in cloud security domains such as architecture, governance, compliance, operations, and data security. Certificate of Cloud Security Knowledge (v4.0) Exam certification program is vendor-neutral and is not tied to any specific cloud service provider, making it an excellent choice for professionals looking to demonstrate their proficiency in cloud security.

The CCSK certification exam covers a wide range of topics related to cloud security, including cloud architecture, governance, compliance, risk management, and data security. CCSK exam consists of 60 multiple-choice questions and must be completed within 90 minutes. Candidates who pass the exam will receive a certificate that demonstrates their knowledge and skills in cloud security.

The New CCSK 2025 Updated Verified Study Guides & Best Courses:
https://www.dumpsmaterials.com/CCSK-real-torrent.html]