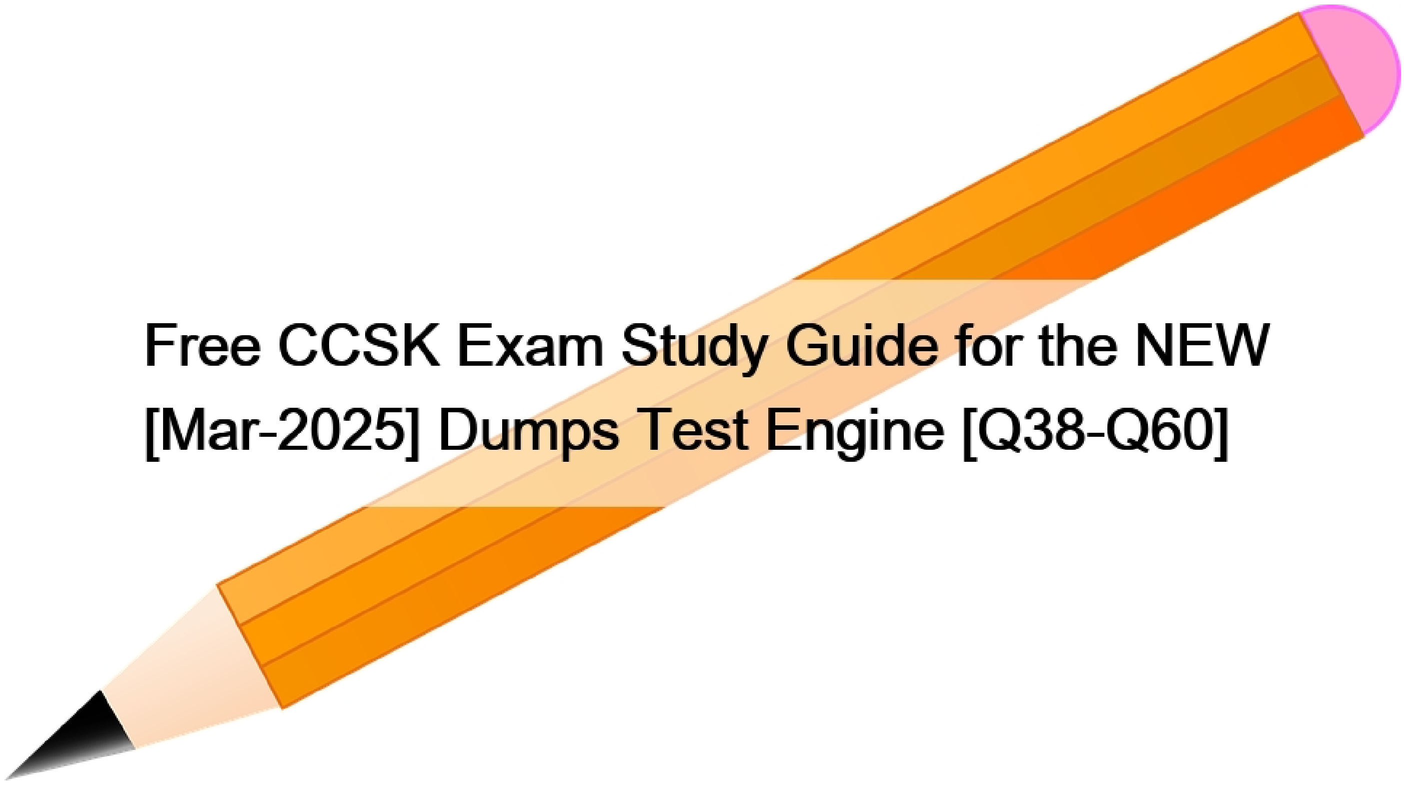
Free CCSK Exam Study Guide for the NEW [Mar-2025 Dumps Test Engine [Q38-Q60



Free CCSK Exam Study Guide for the NEW [Mar-2025 Dumps Test Engine CCSK PDF Dumps Extremely Quick Way Of Preparation

The CCSK certification exam is divided into two parts: the Core exam and the Plus exam. The Core exam covers fundamental cloud security principles and best practices, while the Plus exam goes into greater depth on specific topics such as cloud data security, compliance, and legal issues. CCSK exam is computer-based and can be taken online or in-person at a testing center. CCSK exam is timed and consists of multiple-choice questions, with a passing score of 80%.

Cloud Security Alliance (CSA) Certificate of Cloud Security Knowledge (CCSK) is a globally recognized certification that validates the understanding of foundational cloud security principles and best practices. The CCSK certification is designed for IT and security professionals who work with cloud-based technologies and services or are responsible for managing cloud security. Certificate of Cloud Security Knowledge (v4.0) Exam certification exam covers a broad range of topics, including cloud architecture, infrastructure security, data security, compliance, and legal issues.

Q38. Which of the following is NOT of the essential characterstics as defined by NIST?
* Rapid Elastici
* Resource Sharing
* Resource Pooling

* On-demand self service
All others are characteristics as defined by NIST.

Q39. For third-party audits or attestations, what is critical for providers to publish and customers to evaluate?
* Scope of the assessment and the exact included features and services for the assessment
* Provider infrastructure information including maintenance windows and contracts
* Network or architecture diagrams including all end point security devices in use
* Service-level agreements between all parties
* Full API access to all required services

Q40. Which of the following type of risk assessment most effectively supports cost-benefit analyses of alternative risk responses or courses of action?
* Qualitative Analysis
* Quantitative Analysis
* Third party Risk Analysis
* Outsourced risk analysis
Quantitative assessments typically employ a set of methods, principles, or rules for assessing risk based on the use of numbers This type of assessment most effectively supports cost-benefit analyses of alternative risk responses or courses of action.

Q41. In volume storage, what method is often used to support resiliency and security?
* proxy encryption
* data rights management
* hypervisor agents
* data dispersion
* random placement

Q42. Which statement best describes the impact of Cloud Computing on business continuity management?
* A general lack of interoperability standards means that extra focus must be placed on the security aspects of migration between Cloud providers.
* The size of data sets hosted at a Cloud provider can present challenges if migration to another provider becomes necessary.
* Customers of SaaS providers in particular need to mitigate the risks of application lock-in.
* Clients need to do business continuity planning due diligence in case they suddenly need to switch providers.
* Geographic redundancy ensures that Cloud Providers provide highly available services.

Q43. Where does the encryption engine and key reside when doing file-level encryption?
* On the instance attached to the system
* Encryption engine resides on the server and keys on the client side
* On the KMS attached to the system
* On the client side
File-level encryption: Database servers typically reside on volume storage. For this deployment, you are encrypting the volume or folder of the database, with the encryption engine and keys residing on the instances attached to the volume.

External file system encryption protects from media theft, lost backups, and external attack but does not protect against attacks with access to the application layer, the instances 0S, or the data

Q44. According to CSA Security Guidelines, there are four layers of Logical Model for cloud computing. Which of the following is not one of the layers as defined by Cloud Security Alliance?
* Infrasturcture
* Metastructure
* Applistructure

* Softstructure

The four layers of Logical Model for cloud computing according to Cloud Security Alliance are:

1. Infrastructure: The core components of a computing system: compute, network, and storage. The foundation that everything else is built on. The moving parts.

2. Metastructure: The protocols and mechanisms that provide the interface between the infrastructure layer and the other layers. The glue that ties the technologies and enables management and configuration.

3. Infostructure: The data and information. Content in a database, file storage, etc.

4. Applistructure: The applications deployed in the cloud and the underlying application services used to build them. For example, Platform as a Service features like message queues, artificial intelligence analysis, or notification services.

Q45. Which of the following leverages virtual network topologies to run more. smaller. and more isolated networks without incurring additional hardware costs that historically make such models prohibitive?

* VLANS
* Micro LANs
* Micro segmentation
* BitVLANS

Micro segmentation(also sometimes referred to as hyper segregation) leverages virtual network topologies to run more, smaller, and more isolated networks without incurring additional hardware costs that historically make such models prohibitive. Since the entire networks are defined in software without many of the traditional addressing issues, it is far more feasible to run these multiple, software- defined environments.

Reference: CSA Security GuidelinesV.4(reproduced here for the educational purpose)

Q46. What is the primary focus during the Preparation phase of the Cloud Incident Response framework?

* Developing a cloud service provider evaluation criterion
* Deploying automated security monitoring tools across cloud services
* Establishing a Cloud Incident Response Team and response plans
* Conducting regular vulnerability assessments on cloud infrastructure

The Preparation phase focuses on setting up an incident response team and developing plans to handle incidents efficiently when they occur. Reference: [Security Guidance v5, Domain 11 &#8211; Incident Response]

Q47. &#8220;Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. &#8221; Which of the following characteristics defines this?

* Broad network access
* Resource pooling
* Rapid elasticity
* Measured service

Measured service is defined as &#8220;Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. &#8220;

Q48. What would you call logic/procedures running on a shared database platform as?

* Virtual Machine
* Container
* Platform-based Workload
* Serverless Computing

Platform-based workloads: This is a more complex category that covers workloads running on a shared platform that aren&#8217;t virtual machines or containers, such as logic/procedures running on a shared database platform. Imagine a stored procedure running inside a multitenant database, or a machine- learning job running on a machine-learning Platform as a Service. Isolation and security are totally the responsibility of the platform provider, although the provider may expose certain security options and controls.

Reference: CSA Security GuidelinesV.4(reproduced here for the educational purpose)

Q49. Which communication methods within a cloud environment must be exposed for partners or consumers to access database information using a web application?
* Software Development Kits (SDKs)
* Resource Description Framework (RDF)
* Extensible Markup Language (XML)
* Application Binary Interface (ABI)
* Application Programming Interface (API)

Q50. Which of the following is one of the five essential characteristics of cloud computing as defined by NIST?
* Multi-tenancy
* Nation-state boundaries
* Measured service
* Unlimited bandwidth
* Hybrid clouds

Q51. Lack of standard data formats and service interfaces can lead to:
* Vendor lock out
* Vendor lock in
* Denial of Service
* API Mis-management

Lack of tools, procedures or standard data formats or services interfaces that could guarantee data and service portability, makes it extremely difficult for a customer to migrate from one provider to another, or to migrate data and services to or from an in-House IT environment.

Q52. Which one of the following is not one the cloud deployment models?
* Public
* Private
* Joint
* Community

The four cloud deployment models are

1. Public

2. Private

3. Hybrid

4. Community

Q53. In the context of cloud security, what is the primary benefit of implementing Identity and Access Management (IAM) with attributes and user context for access decisions?
* Enhances security by supporting authorizations based on the current context and status
* Reduces log analysis requirements
* Simplifies regulatory compliance by using a single sign-on mechanism

* These are required for proper implementation of RBAC
Context-aware IAM enables access decisions that account for real-time conditions, enhancing security by adapting to changes in user and resource status. Reference: [CCSK Study Guide, Domain 5 &#8211; IAM]

Q54. What is the primary purpose of the CSA Security, Trust, Assurance, and Risk (STAR) Registry?
* To provide cloud service rate comparisons
* To certify cloud services for regulatory compliance
* To document security and privacy controls of cloud offerings
* To manage data residency and localization requirements
The CSA STAR Registry provides transparency by listing security and privacy controls of CSPs, helping customers assess provider security. Reference: [CCSK Overview, STAR Registry]

Q55. Insufficient Identity. Credential and Access Management can lead to which of the following?
* Spoofing Identity
* Tampering with Data
* Information Disclosure
* All of the above
Sufficient Identity and Access Management practice should be followed in cloud environment.

Weakness in Identity, Credential and Access Management can lead to all types of threats as a compromised credential opens door to complete internal infrastructure.

Q56. Which approach creates a secure network, invisible to unauthorized users?
* Firewalls
* Software-Defined Perimeter (SDP)
* Virtual Private Network (VPN)
* Intrusion Detection System (IDS)
An SDP creates a &#8220;dark&#8221; network, visible only to authorized users, enhancing security by hiding infrastructure from potential attackers. Reference: [Security Guidance v5, Domain 7 &#8211; Infrastructure & Networking]

Q57. All assets require the same continuity in the cloud.
* False
* True

Q58. How can virtual machine communications bypass network security controls?
* VM communications may use a virtual network on the same hardware host
* The guest OS can invoke stealth mode
* Hypervisors depend upon multiple network interfaces
* VM images can contain rootkits programmed to bypass firewalls
* Most network security systems do not recognize encrypted VM traffic

Q59. A unit of processing, which can be in a virtual machine, a container, or other abstraction and always run somewhere on a processor and consume memory is called:
* Host
* Device
* Workload
* Controller
A workload is a unit of processing, which can be in a virtual machine, a container, or other abstraction.

Workloads always run somewhere on a processor and consume memory. Workloads include a very diverse range of processing tasks, which range from traditional applications running in a virtual machine on a standard operating system, to GPU- or FPGA-based specialized tasks Reference: CSA Security Guidelines V.4(reproduced here for the educational purpose)

Q60. Cloud Service Provider and Cloud Customer are jointly responsible for ownership of the all risks in shared responsibility model for security across all service models.
* True
* False
This is false. This is again a tricky question and one should be careful when answering this type of question. It is the cloud customer is who is ultimately responsible for the ownership of risk in the cloud environment. Consumer just passes some of risk management responsibilities to the cloud service provider.

Enhance your career with CCSK PDF Dumps - True Cloud Security Alliance Exam Questions:
https://www.testkingfree.com/Cloud-Security-Alliance/CCSK-practice-exam-dumps.html]