

[Dec 05, 2022 CCSK Free Exam Questions with Quality Guaranteed [Q26-Q47]



[Dec 05, 2022 CCSK Free Exam Questions with Quality Guaranteed CCSK Free Exam Files Downloaded Instantly

Cloud Security Alliance CCSK Foundation Exam Syllabus Topics: **Section Objectives** Management Plane and Business Continuity-Business Continuity and Disaster Recovery in the Cloud

- Architect for Failure
- Management Plane Security Incident Response-Incident Response Lifecycle
- How the Cloud Impacts IR Infrastructure Security-Cloud Network Virtualization
- Security Changes With Cloud Networking
- Challenges of Virtual Appliances
- SDN Security Benefits
- Micro-segmentation and the Software Defined Perimeter

- Hybrid Cloud Considerations
- Cloud Compute and Workload SecurityData Security and Encryption-Data Security Controls
- Cloud Data Storage Types
- Managing Data Migrations to the Cloud
- Securing Data in the CloudRelated Technologies-Big Data
- Internet of Things
- Mobile
- Serverless ComputingGovernance and Enterprise Risk Management-Tools of Cloud Governance
- Enterprise Risk Management in the Cloud
- Effects of various Service and Deployment Models
- Cloud Risk Trade-offs and Tools

NEW QUESTION 26

Which of the following processes leverages virtual network topologies to run more smaller and more isolated networks without incurring additional hardware costs?

- * VLANs
- * Grid networking
- * Micro-segmentation
- * Converged Networking

Explanation:

This type of question are asked to create confusion.

Following are the five phases of SDLC:

1. Planning and requirements analysis: Business and security requirements and standards are being determined. This phase is the main focus of the project managers and stakeholders. Meetings with managers, stakeholders, and users are held to determine requirements. The software development lifecycle calls for all business requirements(functional and nonfunctional)to be defined even before initial design begins. Planning for the quality-assurance requirements and identification of the risks associated with the project are also conducted in the planning stage. The requirements are then analyzed for their validity and the possibility of incorporating them into the system to be developed.

2. Defining: The defining phase is meant to clearly define and document the product requirements to place them in front of the customers and get them approved. This is done through a requirement specification document, which consists of all the product requirements to be designed and developed during the project lifecycle.

3. Designing: System design helps in specifying hardware and system requirements and helps in defining overall system architecture. The system design specifications serve as input for the next phase of the model. Threat modeling and secure design elements should be undertaken and discussed here.

4. Developing: Upon receiving the system design documents, work is divided into modules or units and actual coding starts. This is typically the longest phase of the software development lifecycle. Activities include code review, unit testing, and static analysis.

5. Testing: After the code is developed, it is tested against the requirements to make sure that the product is actually solving the needs gathered during the requirements phase. During this phase, unit testing, integration testing, system testing, and acceptance testing are conducted.

NEW QUESTION 27

Which is the leading industry leading standard you will recommend to a web developer when designing web application or an API for a cloud solution?

- * ISO 27001
- * SOC2
- * FIPS 140
- * OWASP

OWASP is an open project and is leading industry standard for designing web applications and its security.

NEW QUESTION 28

Which statement best describes why it is important to know how data is being accessed?

- * The devices used to access data have different storage formats.
- * The devices used to access data use a variety of operating systems and may have different programs installed on them.
- * The device may affect data dispersion.
- * The devices used to access data use a variety of applications or clients and may have different security characteristics.
- * The devices used to access data may have different ownership characteristics.

NEW QUESTION 29

A health care facility has to only comply with HIPAA and do not need to comply with PCI DSS.

- * True
- * False

This is a tricky question. It is true that health care facility need to comply with HIPAA but if the healthcare facility is processing credit cards, they will have to comply with PCI DSS as well

NEW QUESTION 30

The management plane controls and configures the:

- * Infrastructure
- * Metastructure
- * Infostructure
- * Applistructure

The management plane controls and configures the metastructure and is also part of the metastructure itself. As a reminder, cloud computing is the act of taking physical assets(like networks and processors)and using them to build resource pools. Metastructure is the glue and guts to create, provision, and de-provision the pools. The management plane includes the interfaces for building and managing the cloud itself, but also the interfaces for cloud users to manage their own allocated resources of the cloud.

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

NEW QUESTION 31

In a cloud scenario, who is the data processor and who is the data controller?

- * Cloud Service Provider is the data controller and its customer is the data processor
- * Database admin is the data controller and application owner is the data processor
- * Cloud Service Provider is the data processor and its customer is the data controller
- * Neither cloud service provider nor customer is data processor or data controller.

The customer determines the ultimate purpose of the processing and decides on the outsourcing or the delegation of all or part of the concerned activities to external organizations. Therefore, the customer acts as a controller.

When the service provider supplies the means and the platform, acting on behalf of the customer, it is considered to be a data processor.

NEW QUESTION 32

CCM: In the CCM tool, a is a measure that modifies risk and includes any process, policy, device, practice or any other actions which modify risk.

- * Risk Impact
- * Domain
- * Control Specification

NEW QUESTION 33

Whose responsibility is to maintain security incident and event management (SIEM) capabilities in PaaS (Platform as a Service) model?

- * Cloud Carrier
- * Cloud Service provider
- * Cloud Customer
- * Cloud Access Security Broker

In forms of service models, it is cloud service provider's responsibility to maintain security incident and event management (SIEM) capabilities

NEW QUESTION 34

ISO 27001 certification can be taken as proof to achieve Third-party assessment level in CSA star program.

- * True
- * False

The CSA STAR Certification is a rigorous third-party independent assessment of the security of a cloud service provider. The technology-neutral certification leverages the requirements of the ISO/IEC

27001:2013 management system standard together with the CSA Cloud Controls Matrix.

NEW QUESTION 35

A cloud storage architecture that caches content close to locations of high demand is known as:

- * Volume Data
- * Block Data

- * Ephemeral Storage
- * Content Delivery Network(CDN)

A content delivery network(CDN) is a system of distributed servers(network) that deliver pages and other Web content to a user. based on the geographic locations of the user. the origin of the webpage and the content delivery server.

NEW QUESTION 36

In ability to provide enough capacity to the cloud customer can lead to which of the following risk:

- * Resource Exhaustion
- * Data Breach
- * Resource Utilization
- * Data Dispersion

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 or inadequate resource provisioning and inadequate investments in infrastructure.

NEW QUESTION 37

Which of the following is not an abuse or misuse of cloud services?

- * Launching DDoS Attacks
- * Email Spam
- * Data Deletion
- * Phishing campaigns

Please note here and understand the meaning of phrase '“abuse or misuse of cloud Services”. This phrase means to launch attacks or campaign by using cloud as a platform, mostly, public cloud.

NEW QUESTION 38

Which one of the following is the key techniques to create cloud infrastructure?

- * Authentication
- * Abstraction
- * Orientation
- * Classification

The key techniques to create a cloud are abstraction and orchestration. We abstract the resources from the underlying physical infrastructure to create our pools, and use orchestration (and automation) to coordinate carving out and delivering a set of resources from the pools to the consumers. As you will see, these two techniques create all the essential characteristics we use to define something as a

“cloud.”

Ref: CSA Security Guidelines V4.0

NEW QUESTION 39

Which of the following is also known as white-box test and can be used to find XSS errors, SQL injection.

buffer overflows. unhandled error conditions. and potential backdoors?

- * Threat Modelling
- * Dynamic Application Security Testing(DAST)
- * Static Application Security Testing(SAST)

* **Static Application Security Testing(SAST)**

Static application security testing(SAST) is generally considered a white-box test, where the application test performs an analysis of the application source code, byte code, and binaries without executing the application code. SAST is used to determine coding errors and omissions that are indicative of security vulnerabilities. SAST is often used as a test method while the tool is under development(early in the development lifecycle).

SAST can be used to find XSS errors, SQL injection, buffer overflows, unhandled error conditions, and potential backdoors.

NEW QUESTION 40

All of the following are type of access controls except:

- * Physical
- * Natural
- * Technical
- * Administrative

There is no control as such for Natural control.

There are three types of controls

1. Physical
2. Technical
3. Administrative

NEW QUESTION 41

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 42

Which is the set of technologies that are designed to detect conditions indicative of a security vulnerability in an application in its running state?

- * STRIDE
- * Static application security Testing(SAST)
- * Dynamic application security testing(DAST)
- * Enterprise Threat Modelling

Definitions:

SAST- Static application security testing(SAST) is a type of security testing that relies on inspecting the source code of an application. In general, SAST involves looking at the ways the code is designed to pinpoint possible security flaws.

DAST- Dynamic application security testing(DAST) technologies are designed to detect conditions indicative of a security vulnerability in an application in its running state

NEW QUESTION 43

Which of the following should be your top priority when designing a cloud security program for your organization?

- * Configure IPSEC tunnels
- * Prevention of DDoS Attack
- * Consider OWASP guideline
- * Protection of cloud management plan

In most cases, those APIs are both remotely accessible and wrapped into a web-based user interface.

This combination is the cloud management plane, since consumers use it to manage and configure the cloud resources, such as launching virtual machines (instances) or configuring virtual networks. From a security perspective, it is both the biggest difference from protecting physical infrastructure (since you can't rely on physical access as a control) and the top priority when designing a cloud security program. If an attacker gets into your management plane, they potentially have full remote access to your entire cloud deployment.

Ref: CSA Security Guidelines V4

NEW QUESTION 44

In which cloud service model is the customer only responsible for the data?

- * CaaS
- * SaaS
- * PaaS
- * IaaS

SaaS is the model in which the customer supplies only the data; in the other models, the customer also supplies the OS, the application, or both.

NEW QUESTION 45

Your cloud and on-premises infrastructures should always use the same network address ranges.

- * False
- * True

NEW QUESTION 46

Which of the following Standards define 'Application Security Management Process' (ASMP)?

- * ISO 27032-1
- * ISO 27034-1
- * ISO 27036-1
- * ISO 27038-1

The International Organization for Standardization (ISO) has developed and published ISO/IEC 27034-1,

Information Technology, eSecurity Techniques, eApplication Security, ISO/IEC 27034-1 defines concepts, frameworks, and processes to help organizations integrate security within their software development lifecycle.

NEW QUESTION 47

Your SLA with your cloud provider ensures continuity for all services.

- * False
- * True

Explanation

Average Salary of Certificate of Cloud Security Knowledge (CCSK) Exam Certified Professionals

The average salary of a Certificate of Cloud Security Knowledge (CCSK) Exam Certified Professional is:

- India: 4,477,000 INR- United State: 60,550 USD- Europe: 50,000 EURO- England: 45,000 POUND

Difficulty in Writing Certificate of Cloud Security Knowledge (CCSK) Exam

The Certificate of Cloud Security Knowledge (CCSK) exam is an open book exam. It may be an open-book, but don't underestimate this exam's complexity. The passing rate is 62% for this exam. We find that, depending on their experience, there is no one place where students struggle most. Someone in that segment who has never worked in network security will struggle more while the network security engineer will struggle. As this offers an overview of each of these regions, the best way to plan is to review the CSA Guidance.

Learning everything and then dropping all of it after the exam is over. The cloud travels rapidly, and you have to keep up with it. Just the beginning of your cloud protection journey should be the CCSK. This exam requires lots of practice to complete on time and for writing accurate solutions. Take a deep look into the exam contents and follow the official training courses mentioned in the ?How to study for this exam? section of this document. After taking the online courses, study the **CCSK exam dumps pdf** properly and then test your knowledge and skills by taking the **CCSK practice exams** before appearing for the actual exam.

These practices are intended to produce better preparatory content in such away. This will ensure that the exam is clear with the right focus and the correct material for training. TopExamCollection have the most up-to-date **CCSK exam dumps**, with the aid of these dump aspirants, getting a good understanding of the question pattern being asked in real certification. The military experts check certification-question for all of the adjustments in the course. TopExamCollection often require testing of practice, which proves to be an excellent forum for testing the knowledge collected. To view the study materials, refer to the links below.

Q&As with Explanations Verified & Correct Answers: <https://www.topexamcollection.com/CCSK-vce-collection.html>]