Exam Questions CCSK

Certificate of Cloud Security Knowledge

https://www.2passeasy.com/dumps/CCSK/

NEW QUESTION 1
In the Software-as-a-service relationship, who is responsible for the majority of the security?

A. Application Consumer
B. Database Manager
C. Application Developer
D. Cloud Provider
E. Web Application CISO

Answer: D

NEW QUESTION 2
CCM: Cloud Controls Matrix (CCM) is a completely independent cloud assessment toolkit that does not map any existing standards.

A. True
B. False

Answer: B

NEW QUESTION 3
How is encryption managed on multi-tenant storage?

A. Single key for all data owners
B. One key per data owner
C. Multiple keys per data owner
D. The answer could be A, B, or C depending on the provider
E. C for data subject to the EU Data Protection Directive; B for all others

Answer: B

NEW QUESTION 4
Which of the following encryption methods would be utilized when object storage is used as the back-end for an application?

A. Database encryption
B. Media encryption
C. Asymmetric encryption
D. Object encryption
E. Client/application encryption

Answer: E

NEW QUESTION 5
What is known as a code execution environment running within an operating system that shares and uses the resources of the operating system?

A. Platform-based Workload
B. Pod
C. Abstraction
D. Container
E. Virtual machine

Answer: D

NEW QUESTION 6
CCM: The Architectural Relevance column in the CCM indicates the applicability of the cloud security control to which of the following elements?

A. Service Provider or Tenant/Consumer
B. Physical, Network, Compute, Storage, Application or Data
C. SaaS, PaaS or IaaS

Answer: C

NEW QUESTION 7
Dynamic Application Security Testing (DAST) might be limited or require pre-testing permission from the provider.

A. False
B. True

Answer: B

NEW QUESTION 8
Cloud applications can use virtual networks and other structures, for hyper-segregated environments.

A. False

B. True

Answer: B

NEW QUESTION 9
What is resource pooling?

A. The provider's computing resources are pooled to serve multiple consumers.
B. Internet-based CPUs are pooled to enable multi-threading.
C. The dedicated computing resources of each client are pooled together in a colocation facility.
D. Placing Internet ("cloud") data centers near multiple sources of energy, such as hydroelectric dams.
E. None of the above.

Answer: A

NEW QUESTION 10
How should an SDLC be modified to address application security in a Cloud Computing environment?

A. Integrated development environments
B. Updated threat and trust models
C. No modification is needed
D. Just-in-time compilers
E. Both B and C

Answer: A

NEW QUESTION 10
Which of the following statements best describes an identity federation?

A. A library of data definitions
B. A group of entities which have decided to exist together in a single cloud
C. Identities which share similar attributes
D. Several countries which have agreed to define their identities with similar attributes
E. The connection of one identity repository to another

Answer: E

NEW QUESTION 12
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?

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

Answer: D

NEW QUESTION 15
What does it mean if the system or environment is built automatically from a template?

A. Nothing.
B. It depends on how the automation is configured.
C. Changes made in production are overwritten by the next code or template change.
D. Changes made in test are overwritten by the next code or template change.
E. Changes made in production are untouched by the next code or template change.

Answer: D

NEW QUESTION 20
How does virtualized storage help avoid data loss if a drive fails?

A. Multiple copies in different locations
B. Drives are backed up, swapped, and archived constantly
C. Full back ups weekly
D. Data loss is unavoidable with drive failures
E. Incremental backups daily

Answer: A

NEW QUESTION 24
If the management plane has been breached, you should confirm the templates/configurations for your infrastructure or applications have not also been compromised.

A. False
B. True

Answer: A

NEW QUESTION 29
ENISA: Which is not one of the five key legal issues common across all scenarios:

A. Data protection
B. Professional negligence
C. Globalization
D. Intellectual property
E. Outsourcing services and changes in control

Answer: C

NEW QUESTION 30
Which cloud security model type provides generalized templates for helping implement cloud security?

A. Conceptual models or frameworks
B. Design patterns
C. Controls models or frameworks
D. Reference architectures
E. Cloud Controls Matrix (CCM)

Answer: D

NEW QUESTION 33
Which of the following items is NOT an example of Security as a Service (SecaaS)?

A. Spam filtering
B. Authentication
C. Provisioning
D. Web filtering
E. Intrusion detection

Answer: C

NEW QUESTION 36
When designing an encryption system, you should start with a threat model.

A. False
B. True

Answer: B

NEW QUESTION 37
How can virtual machine communications bypass network security controls?

A. VM communications may use a virtual network on the same hardware host
B. The guest OS can invoke stealth mode
C. Hypervisors depend upon multiple network interfaces
D. VM images can contain rootkits programmed to bypass firewalls
E. Most network security systems do not recognize encrypted VM traffic

Answer: A

NEW QUESTION 38
What are the primary security responsibilities of the cloud provider in the management infrastructure?

A. Building and properly configuring a secure network infrastructure
B. Configuring second factor authentication across the network
C. Properly configuring the deployment of the virtual network, especially the firewalls
D. Properly configuring the deployment of the virtual network, except the firewalls
E. Providing as many API endpoints as possible for custom access and configurations

Answer: D

NEW QUESTION 40
CCM: In the CCM tool, ais a measure that modifies risk and includes any process, policy, device, practice or any other actions which modify risk.

A. Risk Impact
B. Domain
C. Control Specification

Answer: C

NEW QUESTION 41
CCM: In the CCM tool, "Encryption and Key Management" is an example of which of the following?

A. Risk Impact
B. Domain
C. Control Specification

Answer: B

NEW QUESTION 43
Which of the following is a perceived advantage or disadvantage of managing enterprise risk for cloud deployments?

A. More physical control over assets and processes.
B. Greater reliance on contracts, audits, and assessments due to lack of visibility or management.
C. Decreased requirement for proactive management of relationship and adherence to contracts.
D. Increased need, but reduction in costs, for managing risks accepted by the cloud provider.
E. None of the above.

Answer: B

NEW QUESTION 44
For third-party audits or attestations, what is critical for providers to publish and customers to evaluate?

A. Scope of the assessment and the exact included features and services for the assessment
B. Provider infrastructure information including maintenance windows and contracts
C. Network or architecture diagrams including all end point security devices in use
D. Service-level agreements between all parties
E. Full API access to all required services

Answer: C

NEW QUESTION 47
What is the most significant security difference between traditional infrastructure and cloud computing?

A. Management plane
B. Intrusion detection options
C. Secondary authentication factors
D. Network access points
E. Mobile security configuration options

Answer: A

NEW QUESTION 52
When mapping functions to lifecycle phases, which functions are required to successfully process data?

A. Create, Store, Use, and Share
B. Create and Store
C. Create and Use
D. Create, Store, and Use
E. Create, Use, Store, and Delete

Answer: A

NEW QUESTION 56
ENISA: A reason for risk concerns of a cloud provider being acquired is:

A. Arbitrary contract termination by acquiring company
B. Resource isolation may fail
C. Provider may change physical location
D. Mass layoffs may occur
E. Non-binding agreements put at risk

Answer: E

NEW QUESTION 58
When deploying Security as a Service in a highly regulated industry or environment, what should both parties agree on in advance and include in the SLA?

A. The metrics defining the service level required to achieve regulatory objectives.
B. The duration of time that a security violation can occur before the client begins assessing regulatory fines.
C. The cost per incident for security breaches of regulated information.
D. The regulations that are pertinent to the contract and how to circumvent them.
E. The type of security software which meets regulations and the number of licenses that will be needed.

Answer: A

NEW QUESTION 62
To understand their compliance alignments and gaps with a cloud provider, what must cloud customers rely on?

A. Provider documentation
B. Provider run audits and reports
C. Third-party attestations
D. Provider and consumer contracts
E. EDiscovery tools

Answer: C

NEW QUESTION 63
Which communication methods within a cloud environment must be exposed for partners or consumers to access database information using a web application?

A. Software Development Kits (SDKs)
B. Resource Description Framework (RDF)
C. Extensible Markup Language (XML)
D. Application Binary Interface (ABI)
E. Application Programming Interface (API)

Answer: E

NEW QUESTION 64
The Software Defined Perimeter (SDP) includes which components?

A. Client, Controller, and Gateway
B. Client, Controller, Firewall, and Gateway
C. Client, Firewall, and Gateway
D. Controller, Firewall, and Gateway
E. Client, Controller, and Firewall

Answer: A

NEW QUESTION 67
Which statement best describes the Data Security Lifecycle?

A. The Data Security Lifecycle has six stages, is strictly linear, and never varies.
B. The Data Security Lifecycle has six stages, can be non-linear, and varies in that some data may never pass through all stages.
C. The Data Security Lifecycle has five stages, is circular, and varies in that some data may never pass through all stages.
D. The Data Security Lifecycle has six stages, can be non-linear, and is distinct in that data must always pass through all phases.
E. The Data Security Lifecycle has five stages, can be non-linear, and is distinct in that data must always pass through all phases.

Answer: B

NEW QUESTION 68
......

CCSK Practice Exam Features:

* CCSK Questions and Answers Updated Frequently

* CCSK Practice Questions Verified by Expert Senior Certified Staff

* CCSK Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CCSK Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year