Number: CCSK
Passing Score: 800
Time Limit: 120
File Version: 5.0

Exam Code: CCSK
Exam Name: Certificate of Cloud Security Knowledge

Exam A

QUESTION 1
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

Correct Answer: B
Section:

QUESTION 2
Which type of application security testing tests running applications and includes tests such as web vulnerability testing and fuzzing?

A. Code Review
B. Static Application Security Testing (SAST)
C. Unit Testing
D. Functional Testing
E. Dynamic Application Security Testing (DAST)

Correct Answer: E
Section:

QUESTION 3
CCM: The Cloud Service Delivery Model Applicability column in the CCM indicates the applicability of the cloud security control to which of the following elements?

A. Mappings to well-known standards and frameworks
B. Service Provider or Tenant/Consumer
C. Physical, Network, Compute, Storage, Application or Data
D. SaaS, PaaS or IaaS

Correct Answer: D
Section:

QUESTION 4
Any given processor and memory will nearly always be running multiple workloads, often from different tenants.

A. False
B. True

Correct Answer: B

Section:

QUESTION 5
In which deployment model should the governance strategy consider the minimum common set of controls comprised of the Cloud Service Provider contract and the organization's internal governance agreements?

A. Public
B. PaaS
C. Private
D. IaaS
E. Hybrid

Correct Answer: E
Section:

QUESTION 6
Which statement best describes why it is important to know how data is being accessed?

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

Correct Answer: D
Section:

QUESTION 7
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.

Correct Answer: A
Section:

QUESTION 8
Your SLA with your cloud provider ensures continuity for all services.

A. False
B. True

Correct Answer: A
Section:

QUESTION 9
What factors should you understand about the data specifically due to legal, regulatory, and jurisdictional factors?

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

Correct Answer: D
Section:

QUESTION 10
Which cloud-based service model enables companies to provide client-based access for partners to databases or applications?

A. Platform-as-a-service (PaaS)
B. Desktop-as-a-service (DaaS)
C. Infrastructure-as-a-service (IaaS)
D. Identity-as-a-service (IDaaS)
E. Software-as-a-service (SaaS)

Correct Answer: A
Section:

QUESTION 11
CCM: The following list of controls belong to which domain of the CCM?
GRM 06 – Policy
GRM 07 – Policy Enforcement
GRM 08 – Policy Impact on Risk Assessments
GRM 09 – Policy Reviews
GRM 10 – Risk Assessments
GRM 11 – Risk Management Framework

A. Governance and Retention Management
B. Governance and Risk Management
C. Governing and Risk Metrics

Correct Answer: B
Section:

QUESTION 12
Which attack surfaces, if any, does virtualization technology introduce?

A. The hypervisor
B. Virtualization management components apart from the hypervisor
C. Configuration and VM sprawl issues
D. All of the above

Correct Answer: D
Section:

QUESTION 13
APIs and web services require extensive hardening and must assume attacks from authenticated and unauthenticated adversaries.

A. False
B. True

Correct Answer: B
Section:

QUESTION 14
Which of the following is NOT a cloud computing characteristic that impacts incidence response?

A. The on demand self-service nature of cloud computing environments.
B. Privacy concerns for co-tenants regarding the collection and analysis of telemetry and artifacts associated with an incident.
C. The possibility of data crossing geographic or jurisdictional boundaries.
D. Object-based storage in a private cloud.
E. The resource pooling practiced by cloud services, in addition to the rapid elasticity offered by cloud infrastructures.

Correct Answer: B
Section:

QUESTION 15
Big data includes high volume, high variety, and high velocity.

A. False
B. True

Correct Answer: B
Section:

QUESTION 16
CCM: A hypothetical company called: "Health4Sure" is located in the United States and provides cloud based services for tracking patient health. The company is compliant with HIPAA/HITECH Act among other industry standards. Health4Sure decides to assess the overall security of their cloud service against the CCM toolkit so that they will be able to present this document to potential clients. Which of the following approach would be most suitable to assess the overall security posture of Health4Sure's cloud service?

A. The CCM columns are mapped to HIPAA/HITECH Act and therefore Health4Sure could verify the CCM controls already covered ad a result of their compliance with HIPPA/HITECH Act. They could then assess the remaining controls. This approach will save time.
B. The CCM domain controls are mapped to HIPAA/HITECH Act and therefore Health4Sure could verify the CCM controls already covered as a result of their compliance with HIPPA/HITECH Act. They could then assess the remaining controls thoroughly. This approach saves time while being able to assess the company's overall security posture in an efficient manner.
C. The CCM domains are not mapped to HIPAA/HITECH Act. Therefore Health4Sure should assess the security posture of their cloud service against each and every control in the CCM. This approach will allow a thorough assessment of the security posture.

Correct Answer: C
Section:

QUESTION 17

A defining set of rules composed of claims and attributes of the entities in a transaction, which is used to determine their level of access to cloud-based resources is called what?

A. An entitlement matrix
B. A support table
C. An entry log
D. A validation process
E. An access log

Correct Answer: D
Section:

QUESTION 18
Cloud applications can use virtual networks and other structures, for hyper-segregated environments.

A. False
B. True

Correct Answer: B
Section:

QUESTION 19
Your cloud and on-premises infrastructures should always use the same network address ranges.

A. False
B. True

Correct Answer: A
Section:

QUESTION 20
Which layer is the most important for securing because it is considered to be the foundation for secure cloud operations?

A. Infrastructure
B. Datastructure
C. Infostructure
D. Applistructure
E. Metastructure

Correct Answer: A
Section:

QUESTION 21
Why is a service type of network typically isolated on different hardware?

A. It requires distinct access controls
B. It manages resource pools for cloud consumers
C. It has distinct functions from other networks

D. It manages the traffic between other networks
E. It requires unique security

Correct Answer: D
Section:

QUESTION 22
Which governance domain deals with evaluating how cloud computing affects compliance with internal security policies and various legal requirements, such as regulatory and legislative?

A. Legal Issues: Contracts and Electronic Discovery
B. Infrastructure Security
C. Compliance and Audit Management
D. Information Governance
E. Governance and Enterprise Risk Management

Correct Answer: C
Section:

QUESTION 23
An important consideration when performing a remote vulnerability test of a cloud-based application is to

A. Obtain provider permission for test
B. Use techniques to evade cloud provider's detection systems
C. Use application layer testing tools exclusively
D. Use network layer testing tools exclusively
E. Schedule vulnerability test at night

Correct Answer: A
Section:

QUESTION 24
Cloud services exhibit five essential characteristics that demonstrate their relation to, and differences from, traditional computing approaches. Which one of the five characteristics is described as: a consumer can unilaterally provision computing capabilities such as server time and network storage as needed.

A. Rapid elasticity
B. Resource pooling
C. Broad network access
D. Measured service
E. On-demand self-service

Correct Answer: E
Section:

QUESTION 25
REST APIs are the standard for web-based services because they run over HTTPS and work wellacross diverse environments.

A. False

B. True

Correct Answer: B
Section:

QUESTION 26
Which of the following statements are NOT requirements of governance and enterprise risk management in a cloud environment?

A. Inspect and account for risks inherited from other members of the cloud supply chain and take active measures to mitigate and contain risks through operational resiliency.
B. Respect the interdependency of the risks inherent in the cloud supply chain and communicate the corporate risk posture and readiness to consumers and dependent parties.
C. Negotiate long-term contracts with companies who use well-vetted software application to avoid the transient nature of the cloud environment.
D. Provide transparency to stakeholders and shareholders demonstrating fiscal solvency and organizational transparency.
E. Both B and C.

Correct Answer: C
Section:

QUESTION 27
What is defined as the process by which an opposing party may obtain private documents for use in litigation?

A. Discovery
B. Custody
C. Subpoena
D. Risk Assessment
E. Scope

Correct Answer: A
Section:

QUESTION 28
What item below allows disparate directory services and independent security domains to be interconnected?

A. Coalition
B. Cloud
C. Intersection
D. Union
E. Federation

Correct Answer: E
Section:

QUESTION 29
Use elastic servers when possible and move workloads to new instances.

A. False
B. True

Correct Answer: B
Section:

QUESTION 30
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

Correct Answer: C
Section:

QUESTION 31
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.

Correct Answer: B
Section:

QUESTION 32
Which data security control is the LEAST likely to be assigned to an IaaS provider?

A. Application logic
B. Access controls
C. Encryption solutions
D. Physical destruction
E. Asset management and tracking

Correct Answer: A
Section:

QUESTION 33
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

Correct Answer: A
Section:

QUESTION 34
What is the newer application development methodology and philosophy focused on automation of application development and deployment?

A. Agile
B. BusOps
C. DevOps
D. SecDevOps
E. Scrum

Correct Answer: C
Section:

QUESTION 35
Sending data to a provider's storage over an API is likely as much more reliable and secure than setting up your own SFTP server on a VM in the same provider

A. False
B. True

Correct Answer: B
Section:

QUESTION 36
What is true of searching data across cloud environments?

A. You might not have the ability or administrative rights to search or access all hosted data.
B. The cloud provider must conduct the search with the full administrative controls.
C. All cloud-hosted email accounts are easily searchable.
D. Search and discovery time is always factored into a contract between the consumer and provider.
E. You can easily search across your environment using any E-Discovery tool.

Correct Answer: A
Section:

QUESTION 37
How does running applications on distinct virtual networks and only connecting networks as needed help?

A. It reduces hardware costs
B. It provides dynamic and granular policies with less management overhead
C. It locks down access and provides stronger data security
D. It reduces the blast radius of a compromised system
E. It enables you to configure applications around business groups

Correct Answer: D
Section:

QUESTION 38
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

Correct Answer: A
Section:

QUESTION 39
ENISA: "VM hopping" is:

A. Improper management of VM instances, causing customer VMs to be commingled with other customer systems.
B. Looping within virtualized routing systems.
C. Lack of vulnerability management standards.
D. Using a compromised VM to exploit a hypervisor, used to take control of other VMs.
E. Instability in VM patch management causing VM routing errors.

Correct Answer: D
Section:

QUESTION 40
Which concept is a mapping of an identity, including roles, personas, and attributes, to an authorization?

A. Access control
B. Federated Identity Management
C. Authoritative source
D. Entitlement
E. Authentication

Correct Answer: D
Section:

QUESTION 41
Which concept provides the abstraction needed for resource pools?

A. Virtualization
B. Applistructure
C. Hypervisor
D. Metastructure

E. Orchestration

Correct Answer: A
Section:

QUESTION 42
Network logs from cloud providers are typically flow records, not full packet captures.

A. False
B. True

Correct Answer: B
Section:

QUESTION 43
Select the best definition of "compliance" from the options below.

A. The development of a routine that covers all necessary security measures.
B. The diligent habits of good security practices and recording of the same.
C. The timely and efficient filing of security reports.
D. The awareness and adherence to obligations, including the assessment and prioritization of corrective actions deemed necessary and appropriate.
E. The process of completing all forms and paperwork necessary to develop a defensible paper trail.

Correct Answer: D
Section:

QUESTION 44
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

Correct Answer: B
Section:

QUESTION 45
In volume storage, what method is often used to support resiliency and security?

A. proxy encryption
B. data rights management
C. hypervisor agents
D. data dispersion
E. random placement

Correct Answer: D
Section:

QUESTION 46
What is true of security as it relates to cloud network infrastructure?

A. You should apply cloud firewalls on a per-network basis.
B. You should deploy your cloud firewalls identical to the existing firewalls.
C. You should always open traffic between workloads in the same virtual subnet for better visibility.
D. You should implement a default allow with cloud firewalls and then restrict as necessary.
E. You should implement a default deny with cloud firewalls.

Correct Answer: E
Section:

QUESTION 47
Which statement best describes the impact of Cloud Computing on business continuity management?

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

Correct Answer: E
Section:

QUESTION 48
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

Correct Answer: D
Section:

QUESTION 49
Which term is used to describe the use of tools to selectively degrade portions of the cloud to continuously test business continuity?

A. Planned Outages
B. Resiliency Planning
C. Expected Engineering
D. Chaos Engineering
E. Organized Downtime

Correct Answer: D
Section:

QUESTION 50
What is true of companies considering a cloud computing business relationship?

A. The laws protecting customer data are based on the cloud provider and customer location only.
B. The confidentiality agreements between companies using cloud computing services is limited legally to the company, not the provider.
C. The companies using the cloud providers are the custodians of the data entrusted to them.
D. The cloud computing companies are absolved of all data security and associated risks through contracts and data laws.
E. The cloud computing companies own all customer data.

Correct Answer: C
Section:

QUESTION 51
Dynamic Application Security Testing (DAST) might be limited or require pre-testing permission from the provider.

A. False
B. True

Correct Answer: B
Section:

QUESTION 52
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.

Correct Answer: A
Section:

QUESTION 53
Which cloud storage technology is basically a virtual hard drive for instanced or VMs?

A. Volume storage
B. Platform
C. Database
D. Application
E. Object storage

Correct Answer: A
Section:

QUESTION 54
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

Correct Answer: C
Section:

QUESTION 55
Which of the following is NOT normally a method for detecting and preventing data migration into the cloud?

A. Intrusion Prevention System
B. URL filters
C. Data Loss Prevention
D. Cloud Access and Security Brokers (CASB)
E. Database Activity Monitoring

Correct Answer: A
Section:

QUESTION 56
In which type of environment is it impractical to allow the customer to conduct their own audit, making it important that the data center operators are required to provide auditing for the customers?

A. Multi-application, single tenant environments
B. Long distance relationships
C. Multi-tenant environments
D. Distributed computing arrangements
E. Single tenant environments

Correct Answer: C
Section:

QUESTION 57
ENISA: Lock-in is ranked as a high risk in ENISA research, a key underlying vulnerability causing lock in is:

A. Lack of completeness and transparency in terms of use
B. Lack of information on jurisdictions
C. No source escrow agreement
D. Unclear asset ownership
E. Audit or certification not available to customers

Correct Answer: A
Section:

QUESTION 58
What is the best way to ensure that all data has been removed from a public cloud environment including all media such as back-up tapes?

A. Allowing the cloud provider to manage your keys so that they have the ability to access and delete the data from the main and back-up storage.
B. Maintaining customer managed key management and revoking or deleting keys from the key management system to prevent the data from being accessed again.
C. Practice Integration of Duties (IOD) so that everyone is able to delete the encrypted data.
D. Keep the keys stored on the client side so that they are secure and so that the users have the ability to delete their own data.
E. Both B and D.

Correct Answer: B
Section:

QUESTION 59
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

Correct Answer: E
Section:

QUESTION 60
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)

Correct Answer: E
Section:

QUESTION 61
Containers are highly portable code execution environments.

A. False
B. True

Correct Answer: B
Section:

QUESTION 62
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.

Correct Answer: B
Section:

QUESTION 63
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

Correct Answer: E
Section:

QUESTION 64
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

Correct Answer: D
Section:

QUESTION 65
What method can be utilized along with data fragmentation to enhance security?

A. Encryption
B. Organization
C. Knowledge management
D. IDS
E. Insulation

Correct Answer: E
Section:

QUESTION 66
Which of the following statements best defines the "authorization" as a component of identity, entitlement, and access management?

A. The process of specifying and maintaining access policies
B. Checking data storage to make sure it meets compliance requirements
C. Giving a third party vendor permission to work on your cloud solution
D. Establishing/asserting the identity to the application
E. Enforcing the rules by which access is granted to the resources

Correct Answer: D
Section:

QUESTION 67
How can web security as a service be deployed for a cloud consumer?

A. By proxying or redirecting web traffic to the cloud provider
B. By utilizing a partitioned network drive
C. On the premise through a software or appliance installation
D. Both A and C
E. None of the above

Correct Answer: A
Section:

QUESTION 68
When configured properly, logs can track every code, infrastructure, and configuration change and connect it back to the submitter and approver, including the test results.

A. False
B. True

Correct Answer: B
Section:

QUESTION 69
What of the following is NOT an essential characteristic of cloud computing?

A. Broad Network Access
B. Measured Service
C. Third Party Service
D. Rapid Elasticity
E. Resource Pooling

Correct Answer: C
Section:

QUESTION 70
Without virtualization, there is no cloud.

A. False
B. True

Correct Answer: B
Section:

QUESTION 71
All assets require the same continuity in the cloud.

A. False
B. True

Correct Answer: A
Section:

QUESTION 72
What is known as the interface used to connect with the metastructure and configure the cloud environment?

A. Administrative access
B. Management plane
C. Identity and Access Management
D. Single sign-on
E. Cloud dashboard

Correct Answer: B
Section:

QUESTION 73
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.

Correct Answer: D
Section:
Explanation:

QUESTION 74
CCM: Cloud Controls Matrix (CCM) is a completely independent cloud assessment toolkit that does not map any existing standards.

A. True
B. False

Correct Answer: B
Section: