Vendor: CSA

Exam Code: CCSK

Exam Name: Certificate Of Cloud Security Knowledge

Version: DEMO

QUESTION 1
All cloud services utilize virtualization technologies.

A. False
B. True

Answer: B
Explanation:
As mentioned in the introduction, cloud computing is fundamentally based on virtualization: It's how we abstract resources to create pools. Without virtualization, there is no cloud.

QUESTION 2
If there are gaps in network logging data, what can you do?

A. Nothing. There are simply limitations around the data that can be logged in the cloud.
B. Ask the cloud provider to open more ports.
C. You can instrument the technology stack with your own logging.
D. Ask the cloud provider to close more ports.
E. Nothing. The cloud provider must make the information available.

Answer: C
Explanation:
Where there are gaps you can sometimes instrument the technology stack with your own logging. This can work within instances, containers, and application code in order to gain telemetry important for the investigation. Pay particular attention to PaaS and serverless application architectures; you will likely need to add custom application-level logging.

QUESTION 3
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.

A. Risk Impact
B. Domain
C. Control Specification

Answer: C
Explanation:
Control specification determines the risk.

QUESTION 4
Who is responsible for the security of the physical infrastructure and virtualization platform?

A. The cloud consumer
B. The majority is covered by the consumer
C. It depends on the agreement
D. The responsibility is split equally
E. The cloud provider

Answer: E
Explanation:

The cloud provider will always be responsible for securing the physical infrastructure and the virtualization platform itself.

QUESTION 5
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

Answer: A
Explanation:
Due to all the potential regulatory, contractual, and other jurisdictional issues, it is extremely important to understand both the logical and physical locations of data.

QUESTION 6
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)

Answer: A
Explanation:
Platform as a Service (PaaS) abstracts and provides development or application platforms,such as databases, application platforms.

QUESTION 7
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

Answer: B
Explanation:
GRM-08 "Governance and Risk Management: Policy Impact on Risk Assessments"
GRM-09: "Governance and Risk Management: Policy Reviews"
GRM-10 "Governance and Risk Management: Risk Assessments"
GRM-11 "Governance and Risk Management: Risk Management Framework"

QUESTION 8
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

Answer: D
Explanation:
VM(Virtual Machine) run on host machine hence, Virtual machine attacks have targets that are attacked as follows.
- VM snpashot and virtual image attack
- Virtualization administrator attack
- Virtual network attack
- Virtual security software issues.

QUESTION 9
APIs and web services require extensive hardening and must assume attacks from authenticated and unauthenticated adversaries.

A. False
B. True

Answer: B
Explanation:
APIs and web services need to be extensively hardened and assume attacks from both authenticated and unauthenticated adversaries. This includes using industry standard authentication designed specifically for APIs.

QUESTION 10
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.

Answer: D
Explanation:
Object-based storage in a private cloud is not directly related to incident response. It is a storage architecture that organizes data into discrete objects and is commonly used in cloud storage systems. While it can have implications for data management and accessibility, it does not directly impact incident response processes.

QUESTION 11
Big data includes high volume, high variety, and high velocity.

A. False
B. True

Answer: B
Explanation:
Big data is high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization.

QUESTION 12
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.

Answer: B
Explanation:
CCM, which is part of the CSA Governance, Risk and Compliance (GRC) Stack, is mapped to multiple industry standards, regulations and frameworks that enterprises must follow, including ISO 27001/27002, PCI DSS, HIPAA and COBIT.

QUESTION 13
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

Answer: A
Explanation:
The mapping of an identity to an authorization should be documented in an entitlement matrix. That document outlines the various resources and functions allowed to be used by specific users, groups and roles.

QUESTION 14
Cloud applications can use virtual networks and other structures, for hyper-segregated
environments.

A. False
B. True

Answer: B
Explanation:
Isolated environments. Cloud applications can also leverage virtual networks and other
structures, including PaaS, for hyper-segregated environments. For example, it is possible, at no
additional cost, to deploy multiple application stacks on entirely separate virtual networks,
eliminating the ability for an attacker to use one compromised application to attack others behind
the perimeter firewalls.

QUESTION 15
Your cloud and on-premises infrastructures should always use the same network address ranges.

A. False
B. True

Answer: A
Explanation:
With Hybrid Cloud Considerations, If the cloud uses the same network address range as your on-
premises assets, it is effectively unusable.

QUESTION 16
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

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

QUESTION 17
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

Answer: C
Explanation:
A service type of network often serves a specific purpose or function that is different from other networks within a cloud environment. Isolating it on different hardware allows for better control and management of resources dedicated to that particular network. By separating it from other networks, it becomes easier to allocate resources, optimize performance, and apply specific configurations or settings tailored to the unique requirements of that network. This isolation helps prevent interference or conflicts between different network types, ensuring efficient and reliable operation of each network within the cloud environment.

QUESTION 18
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

Answer: C
Explanation:
Maintaining and proving compliance when using cloud computing. Issues dealing with evaluating how cloud computing affects compliance with internal security policies, as well as various compliance requirements (regulatory, legislative, and otherwise) are discussed here. This domain includes some direction on proving compliance during an audit.

QUESTION 19
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

Answer: A
Explanation:
You should determine whether your provider allows customers to perform a VA of their systems. If they don't, and you do it, you may find yourself blocked, because the provider won't know the source of the scan, which could be coming from bad actors.

QUESTION 20
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

Answer: E
Explanation:
On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider. (NIST Definition)

QUESTION 21
REST APIs are the standard for web-based services because they run over HTTPS and work well across diverse environments.

A. False
B. True

Answer: B
Explanation:
APIs have become the standard for web-based services since they run over HTTP/S ans thus work well across diverse evnvironments.

QUESTION 22
What item below allows disparate directory services and independent security domains to be interconnected?

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

Answer: E
Explanation:
Federation is the primary tool used to manage this problem, by building trust relationships between organizations and enforcing them through standards-based technologies.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: ASTR14