Certificate of Cloud Security Knowledge

1. All cloud services utilize virtualization technologies.

A. False

B. True

Answer(s): B

---

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(s): C

---

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

A. Risk Impact

B. Domain

C. Control Speci cation

Answer(s): C

---

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(s): E

---

5. What factors should you understand about the data speci cally 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(s): A

---

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(s): A

---

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(s): B

---

8. Which attack surfaces, if any, does virtualization technology introduce?

A. The hypervisor

B. Virtualization management components apart from the hypervisor

C. Con guration and VM sprawl issues

D. All of the above

Answer(s): D

---

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

A. False

B. True

Answer(s): B

---

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(s): B

---

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

A. False

B. True

Answer(s): B

---

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 e cient 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(s): C

---

13. A de ning 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(s): D

---

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

A. False

B. True

Answer(s): B

---

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

A. False

B. True

Answer(s): A

---

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(s): A

---

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 tra c between other networks

E. It requires unique security

Answer(s): D

---

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(s): C

---

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(s): A

20. Cloud services exhibit ve essential characteristics that demonstrate their relation to, and differences from, traditional computing approaches.
Which one of the ve 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(s): E