

**QUESTION 117**

Which type of testing uses the same strategies and toolsets that hackers would use?

- A. Penetration
- B. Dynamic
- C. Static
- D. Malicious

**Correct Answer: A**

**Explanation:**

Penetration testing involves using the same strategies and toolsets that hackers would use against a system to discovery potential vulnerabilities.

**QUESTION 118**

From a security perspective, which of the following is a major concern when evaluating possible BCDR solutions?

- A. Access provisioning
- B. Auditing
- C. Jurisdictions
- D. Authorization

**Correct Answer: C**

**Explanation:**

When a security professional is considering cloud solutions for BCDR, a top concern is the jurisdiction where the cloud systems are hosted. If the jurisdiction is different from where the production systems are hosted, they may be subjected to different regulations and controls, which would make a seamless BCDR solution far more difficult.

**QUESTION 119**

Which of the following is NOT a focus or consideration of an internal audit?

- A. Certification
- B. Design
- C. Costs
- D. Operational efficiency

**Correct Answer: A**

**Explanation:**

In order to obtain and comply with certifications, independent external audits must be performed and satisfied. Although some testing of certification controls can be part of an internal audit, they will not satisfy requirements.

**QUESTION 120**

Which of the following is the sole responsibility of the cloud customer, regardless of which cloud model is used?

- A. Infrastructure
- B. Platform
- C. Application
- D. Data

**[Download Full Version CCSP Exam Dumps\(Updated in Feb/2023\)](#)**

**Correct Answer:** D

**Explanation:**

Regardless of which cloud-hosting model is used, the cloud customer always has sole responsibility for the data and its security.

**QUESTION 121**

What process is used within a clustered system to provide high availability and load balancing?

- A. Dynamic balancing
- B. Dynamic clustering
- C. Dynamic optimization
- D. Dynamic resource scheduling

**Correct Answer:** D

**Explanation:**

Dynamic resource scheduling (DRS) is used within all clustering systems as the method for clusters to provide high availability, scaling, management, and workload distribution and balancing of jobs and processes. From a physical infrastructure perspective, DRS is used to balance compute loads between physical hosts in a cloud to maintain the desired thresholds and limits on the physical hosts.

**QUESTION 122**

Which of the following is NOT a function performed by the handshake protocol of TLS?

- A. Key exchange
- B. Encryption
- C. Negotiation of connection
- D. Establish session ID

**Correct Answer:** B

**Explanation:**

The handshake protocol negotiates and establishes the connection as well as handles the key exchange and establishes the session ID. It does not perform the actual encryption of data packets.

**QUESTION 123**

Unlike SOC Type 1 reports, which are based on a specific point in time, SOC Type 2 reports are done over a period of time. What is the minimum span of time for a SOC Type 2 report?

- A. Six months
- B. One month
- C. One year
- D. One week

**Correct Answer:** A

**Explanation:**

SOC Type 2 reports are focused on the same policies and procedures, as well as their effectiveness, as SOC Type 1 reports, but are evaluated over a period of at least six consecutive months, rather than a finite point in time.

**QUESTION 124**

**[CCSP Exam Dumps](#)   **[CCSP PDF Dumps](#)   **[CCSP VCE Dumps](#)   **[CCSP Q&As](#)********

**<https://www.ensurepass.com/CCSP.html>**

[Download Full Version CCSP Exam Dumps\(Updated in Feb/2023\)](#)

What changes are necessary to application code in order to implement DNSSEC?

- A. Adding encryption modules
- B. Implementing certificate validations
- C. Additional DNS lookups
- D. No changes are needed.

**Correct Answer: D**

**Explanation:**

To implement DNSSEC, no additional changes are needed to applications or their code because the integrity checks are all performed at the system level.

**QUESTION 125**

Which type of controls are the SOC Type 1 reports specifically focused on?

- A. Integrity
- B. PII
- C. Financial
- D. Privacy

**Correct Answer: C**

**Explanation:**

SOC Type 1 reports are focused specifically on internal controls as they relate to financial reporting.

**QUESTION 126**

Which security concept is based on preventing unauthorized access to data while also ensuring that it is accessible to those authorized to use it?

- A. Integrity
- B. Availability
- C. Confidentiality
- D. Nonrepudiation

**Correct Answer: C**

**Explanation:**

The main goal of confidentiality is to ensure that sensitive information is not made available or leaked to parties that should not have access to it, while at the same time ensuring that those with appropriate need and authorization to access it can do so in a manner commensurate with their needs and confidentiality requirements.

**QUESTION 127**

Which of the following is NOT a domain of the Cloud Controls Matrix (CCM)?

- A. Data center security
- B. Human resources
- C. Mobile security
- D. Budgetary and cost controls

**Correct Answer: D**

**Explanation:**

Budgetary and cost controls is not one of the domains outlined in the CCM.

[CCSP Exam Dumps](#)   [CCSP PDF Dumps](#)   [CCSP VCE Dumps](#)   [CCSP Q&As](#)

<https://www.ensurepass.com/CCSP.html>

**QUESTION 128**

Which security concept, if implemented correctly, will protect the data on a system, even if a malicious actor gains access to the actual system?

- A. Sandboxing
- B. Encryption
- C. Firewalls
- D. Access control

**Correct Answer: B**

**Explanation:**

In any environment, data encryption is incredibly important to prevent unauthorized exposure of data either internally or externally. If a system is compromised by an attack, having the data encrypted on the system will prevent its unauthorized exposure or export, even with the system itself being exposed.

**QUESTION 129**

Which of the following is the sole responsibility of the cloud provider, regardless of which cloud model is used?

- A. Platform
- B. Data
- C. Physical environment
- D. Infrastructure

**Correct Answer: C**

**Explanation:**

Regardless of which cloud-hosting model is used, the cloud provider always has sole responsibility for the physical environment.

**QUESTION 130**

Which of the following is NOT a factor that is part of a firewall configuration?

- A. Encryption
- B. Port
- C. Protocol
- D. Source IP

**Correct Answer: A**

**Explanation:**

Firewalls take into account source IP, destination IP, the port the traffic is using, as well as the network protocol (UDP/TCP). Whether or not the traffic is encrypted is not something a firewall is concerned with.

**QUESTION 131**

Which of the cloud deployment models involves spanning multiple cloud environments or a mix of cloud hosting models?

- A. Community
- B. Public

- C. Hybrid
- D. Private

**Correct Answer: C**

**Explanation:**

A hybrid cloud model involves the use of more than one type of cloud hosting models, typically the mix of private and public cloud hosting models.

**QUESTION 132**

Which of the following is NOT one of five principles of SOC Type 2 audits?

- A. Privacy
- B. Processing integrity
- C. Financial
- D. Security

**Correct Answer: C**

**Explanation:**

The SOC Type 2 audits include five principles: security, privacy, processing integrity, availability, and confidentiality.

**QUESTION 133**

Which aspect of cloud computing makes data classification even more vital than in a traditional data center?

- A. Interoperability
- B. Virtualization
- C. Multitenancy
- D. Portability

**Correct Answer: C**

**Explanation:**

With multiple tenants within the same hosting environment, any failure to properly classify data may lead to potential exposure to other customers and applications within the same environment.

**QUESTION 134**

What concept does the "T" represent in the STRIDE threat model?

- A. TLS
- B. Testing
- C. Tampering with data
- D. Transport

**Correct Answer: C**

**Explanation:**

Any application that sends data to the user will face the potential that the user could manipulate or alter the data, whether it resides in cookies, GET or POST commands, or headers, or manipulates client-side validations. If the user receives data from the application, it is crucial that the application validate and verify any data that is received back from the user.

**QUESTION 135**

[CCSP Exam Dumps](#)   [CCSP PDF Dumps](#)   [CCSP VCE Dumps](#)   [CCSP Q&As](#)

<https://www.ensurepass.com/CCSP.html>