DUMPSARENA

Certified Cloud Security Professional (CCSP)

ISC2 CCSP

Version Demo

Total Demo Questions: 12

Total Premium Questions: 860

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

What aspect of a Type 2 hypervisor involves additional security concerns that are not relevant with a Type 1 hypervisor?
Response:

A. Reliance on a host operating system

B. Auditing

C. Proprietary software

D. Programming languages

ANSWER: A

Explanation:

QUESTION NO: 2

Which value refers to the percentage of production level restoration needed to meet BCDR objectives?

A. RPO

B. RTO

C. RSL

D. SRE

ANSWER: C

Explanation:

The recovery service level (RSL) is a percentage measure of the total typical production service level that needs to be restored to meet BCDR objectives in the case of a failure.

QUESTION NO: 3

Which SSAE 16 report is purposefully designed for public release (for instance, to be posted on a company's website)?
Response:

A. SOC 1

B. SOC 2, Type 1

C. SOC 2, Type 2

D. SOC 3

ANSWER: D

Explanation:

QUESTION NO: 4

What are the objectives of change management? (Choose all that apply.) Response:

A. Respond to a customer's changing business requirements while maximizing value and reducing incidents, disruption, and rework

B. Ensure that changes are recorded and evaluated

C. Respond to business and IT requests for change that will disassociate services with business needs

D. Ensure that all changes are prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner

ANSWER: A B

Explanation:

QUESTION NO: 5

Clustered systems can be used to ensure high availability and load balancing across individual systems through a variety of methodologies.

What process is used within a clustered system to ensure proper load balancing and to maintain the health of the overall system to provide high availability?

A. Distributed clustering

B. Distributed balancing

C. Distributed optimization

D. Distributed resource scheduling

ANSWER: D

Explanation:

Distributed resource scheduling (DRS) is used within all clustered systems as the method for providing high availability, scaling, management, workload distribution, and the balancing of jobs and processes. None of the other choices is the correct term in this case.

QUESTION NO: 6

Hardening the operating system refers to all of the following except:

A. Limiting administrator access

B. Closing unused ports

C. Removing antimalware agents

D. Removing unnecessary services and libraries

ANSWER: C

Explanation:

Removing antimalware agents. Hardening the operating system means making it more secure. Limiting administrator access, closing unused ports, and removing unnecessary services and libraries all have the potential to make an OS more secure. But removing antimalware agents would actually make the system less secure. If anything, antimalware agents should be added, not removed.

QUESTION NO: 7

Which of the following are contractual components that the CSP should review and understand fully when contracting with a cloud service provider?

(Choose two.)

A. Concurrently maintainable site infrastructure

B. Use of subcontractors

C. Redundant site infrastructure capacity components

D. Scope of processing

ANSWER: B D

QUESTION NO: 8

Humidity levels for a data center are a prime concern for maintaining electrical and computing resources properly as well as ensuring that conditions are optimal for top performance.

Which of the following is the optimal humidity level, as established by ASHRAE?

A. 20 to 40 percent relative humidity

B. 50 to 75 percent relative humidity

C. 40 to 60 percent relative humidity

D. 30 to 50 percent relative humidity

ANSWER: C

Explanation:

The American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE) recommends 40 to 60 percent relatively humidity for data centers. None of these options is the recommendation from ASHRAE.

QUESTION NO: 9

BCDR strategies typically do not involve the entire operations of an organization, but only those deemed critical to their business.

Which concept pertains to the required amount of time to restore services to the predetermined level?

A. RPO

B. RSL

C. RTO

D. SRE

ANSWER: C

Explanation:

The recovery time objective (RTO) measures the amount of time necessary to recover operations to meet the BCDR plan. The recovery service level (RSL) measures the percentage of operations that would be recovered during a BCDR situation. The recovery point objective (RPO) sets and defines the amount of data an organization must have available or accessible to reach the predetermined level of operations necessary during a BCDR situation. SRE is provided as an erroneous response.

QUESTION NO: 10

In attempting to provide a layered defense, the security practitioner should convince senior management to include security controls of which type?

A. Physical

B. All of the above

C. technological

D. Administrative

ANSWER: B

Explanation:

Layered defense calls for a diverse approach to security.

QUESTION NO: 11

Which of the following is not typically included in the list of critical assets specified for continuity during BCDR contingency operations?

Response:

A. Systems

B. Data

C. Cash

D. Personnel

ANSWER: C

Explanation:

QUESTION NO: 12

Although host-based and network-based IDSs perform similar functions and have similar capabilities, which of the following is an advantage of a network-based IDS over a host-based IDS, assuming all capabilities are equal?

A. Segregated from host systems

B. Network access

C. Scalability

D. External to system patching

ANSWER: A

Explanation:

A network-based IDS has the advantage of being segregated from host systems, and as such, it would not be open to compromise in the same manner a host-based system would be. Although a network-based IDS would be external to system patching, this is not the best answer here because it is a minor concern compared to segregation due to possible host

compromise. Scalability is also not the best answer because, although a network-based IDS does remove processing from the host system, it is not a primary security concern. Network access is not a consideration because both a host-based IDS and a network-based IDS would have access to network resources.