Vendor: ISC

Exam Code: CCSP

Exam Name: Certified Cloud Security Professional (CCSP)

Version: 13.01

Q & As: 409

QUESTION 1
Which of the following roles is responsible for creating cloud components and the testing and validation of services?

A. Cloud auditor
B. Inter-cloud provider
C. Cloud service broker
D. Cloud service developer

Correct Answer: D
Explanation:
The cloud service developer is responsible for developing and creating cloud components and services, as well as for testing and validating services.

QUESTION 2
What is the best source for information about securing a physical asset's BIOS?

A. Security policies
B. Manual pages
C. Vendor documentation
D. Regulations

Correct Answer: C
Explanation:
Vendor documentation from the manufacturer of the physical hardware is the best source of best practices for securing the BIOS.

QUESTION 3
Which of the following is not a component of contractual PII?

A. Scope of processing
B. Value of data
C. Location of data
D. Use of subcontractors

Correct Answer: C
Explanation:
The value of data itself has nothing to do with it being considered a part of contractual

QUESTION 4
Which of the following concepts refers to a cloud customer paying only for the resources and offerings they use within a cloud environment, and only for the duration that they are consuming them?

A. Consumable service
B. Measured service
C. Billable service
D. Metered service

Correct Answer: B
Explanation:
Measured service is where cloud services are delivered and billed in a metered way, where the cloud customer only pays for those that they actually use, and for the duration of time that they

use them.

QUESTION 5
Which of the following roles involves testing, monitoring, and securing cloud services for an organization?

A. Cloud service integrator
B. Cloud service business manager
C. Cloud service user
D. Cloud service administrator

Correct Answer: D
Explanation:
The cloud service administrator is responsible for testing cloud services, monitoring services, administering security for services, providing usage reports on cloud services, and addressing problem reports.

QUESTION 6
What is the only data format permitted with the SOAP API?

A. HTML
B. SAML
C. XSML
D. XML

Correct Answer: D
Explanation:
The SOAP protocol only supports the XML data format.

QUESTION 7
Which data formats are most commonly used with the REST API?

A. JSON and SAML
B. XML and SAML
C. XML and JSON
D. SAML and HTML

Correct Answer: C
Explanation:
JavaScript Object Notation (JSON) and Extensible Markup Language (XML) are the most commonly used data formats for the Representational State Transfer (REST) API, and are typically implemented with caching for increased scalability and performance.

QUESTION 8
Which of the following threat types involves an application that does not validate authorization for portions of itself after the initial checks?

A. Injection
B. Missing function-level access control
C. Cross-site request forgery
D. Cross-site scripting

Correct Answer: B
Explanation:
It is imperative that an application perform checks when each function or portion of the application is accessed, to ensure that the user is properly authorized to access it. Without continual checks each time a function is accessed, an attacker could forge requests to access portions of the application where authorization has not been granted.

QUESTION 9
Which of the following roles involves overseeing billing, purchasing, and requesting audit reports for an organization within a cloud environment?

A. Cloud service user
B. Cloud service business manager
C. Cloud service administrator
D. Cloud service integrator

Correct Answer: B
Explanation:
The cloud service business manager is responsible for overseeing business and billing administration, purchasing cloud services, and requesting audit reports when necessary

QUESTION 10
What is the biggest concern with hosting a key management system outside of the cloud environment?

A. Confidentiality
B. Portability
C. Availability
D. Integrity

Correct Answer: C
Explanation:
When a key management system is outside of the cloud environment hosting the application, availability is a primary concern because any access issues with the encryption keys will render the entire application unusable.

QUESTION 11
Which of the following approaches would NOT be considered sufficient to meet the requirements of secure data destruction within a cloud environment?

A. Cryptographic erasure
B. Zeroing
C. Overwriting
D. Deletion

Correct Answer: D
Explanation:
Deletion merely removes the pointers to data on a system; it does nothing to actually remove and sanitize the data. As such, the data remains in a recoverable state, and more secure methods are needed to ensure it has been destroyed and is not recoverable by another party.

QUESTION 12