

QUESTION 32

Which of the following APIs are most commonly used within a cloud environment?

- A. REST and SAML
- B. SOAP and REST
- C. REST and XML
- D. XML and SAML

Correct Answer: B

Explanation:

Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) are the most commonly used APIs within a cloud environment. Extensible Markup Language (XML) and Security Assertion Markup Language (SAML) are both standards for exchanging encoded data between two parties, with XML being for more general use and SAML focused on authentication and authorization data.

QUESTION 33

Which of the following attempts to establish an international standard for eDiscovery processes and best practices?

- A. ISO/IEC 31000
- B. ISO/IEC 27050
- C. ISO/IEC 19888
- D. ISO/IEC 27001

Correct Answer: B

Explanation:

ISO/IEC 27050 strives to establish an internationally accepted standard for eDiscovery processes and best practices. It encompasses all steps of the eDiscovery process: identification, preservation, collection, processing, review, analysis, and the final production of the requested data.

QUESTION 34

Which of the following roles is responsible for obtaining new customers and securing contracts and agreements?

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

Correct Answer: B

Explanation:

The cloud service broker is responsible for obtaining new customers, analyzing the marketplace, and securing contracts and agreements.

QUESTION 35

Which term relates to the application of scientific methods and practices to evidence?

- A. Forensics

- B. Methodical
- C. Theoretical
- D. Measured

Correct Answer: A

Explanation:

Forensics is the application of scientific and methodical processes to identify, collect, preserve, analyze, and summarize/report digital information and evidence.

QUESTION 36

Which of the following roles involves the provisioning and delivery of cloud services?

- A. Cloud service deployment manager
- B. Cloud service business manager
- C. Cloud service manager
- D. Cloud service operations manager

Correct Answer: C

Explanation:

The cloud service manager is responsible for the delivery of cloud services, the provisioning of cloud services, and the overall management of cloud services.

QUESTION 37

What is the primary reason that makes resolving jurisdictional conflicts complicated?

- A. Different technology standards
- B. Costs
- C. Language barriers
- D. Lack of international authority

Correct Answer: D

Explanation:

With international operations, systems ultimately cross many jurisdictional boundaries, and many times, they conflict with each other. The major hurdle to overcome for an organization is the lack of an ultimate international authority to mediate such conflicts, with a likely result of legal efforts in each jurisdiction.

QUESTION 38

GAAPs are created and maintained by which organization?

- A. ISO/IEC
- B. AICPA
- C. PCI Council
- D. ISO

Correct Answer: B

Explanation:

The AICPA is the organization responsible for generating and maintaining what are the Generally Accepted Accounting Practices in the United States.

QUESTION 39

Which of the following roles is responsible for preparing systems for the cloud, administering and monitoring services, and managing inventory and assets?

- A. Cloud service business manager
- B. Cloud service deployment manager
- C. Cloud service operations manager
- D. Cloud service manager

Correct Answer: C

Explanation:

The cloud service operations manager is responsible for preparing systems for the cloud, administering and monitoring services, providing audit data as requested or required, and managing inventory and assets.

QUESTION 40

Which protocol allows a system to use block-level storage as if it was a SAN, but over TCP network traffic instead?

- A. SATA
- B. iSCSI
- C. TLS
- D. SCSI

Correct Answer: B

Explanation:

iSCSI is a protocol that allows for the transmission and use of SCSI commands and features over a TCP-based network. iSCSI allows systems to use block-level storage that looks and behaves as a SAN would with physical servers, but to leverage the TCP network within a virtualized environment and cloud.

QUESTION 41

Which of the cloud deployment models is used by popular services such as iCloud, Dropbox, and OneDrive?

- A. Hybrid
- B. Public
- C. Private
- D. Community

Correct Answer: B

Explanation:

Popular services such as iCloud, Dropbox, and OneDrive are all publicly available and are open to any user for free, with possible add-on services offered for a cost.

QUESTION 42

Why does a Type 2 hypervisor typically offer less security control than a Type 1 hypervisor?

- A. A Type 2 hypervisor runs on top of another operating system and is dependent on the security of the OS for its own security.
- B. A Type 2 hypervisor allows users to directly perform some functions with their own access.
- C. A Type 2 hypervisor is open source, so attackers can more easily find exploitable vulnerabilities

with that access.

D. A Type 2 hypervisor is always exposed to the public Internet for federated identity access.

Correct Answer: A

Explanation:

A Type 2 hypervisor differs from a Type 1 hypervisor in that it runs on top of another operating system rather than directly tied into the underlying hardware of the virtual host servers. With this type of implementation, additional security and architecture concerns come into play because the interaction between the operating system and the hypervisor becomes a critical link. The hypervisor no longer has direct interaction and control over the underlying hardware, which means that some performance will be lost due to the operating system in the middle needing its own resources, patching requirements, and operational oversight.

QUESTION 43

Which is the appropriate phase of the cloud data lifecycle for determining the data's classification?

- A. Create
- B. Use
- C. Share
- D. Store

Correct Answer: A

Explanation:

Any time data is created, modified, or imported, the classification needs to be evaluated and set from the earliest phase to ensure security is always properly maintained for the duration of its lifecycle.

QUESTION 44

Which of the following is the optimal temperature for a data center, per the guidelines established by the America Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE)?

- A. 69.8-86.0degF (21-30degC)
- B. 64.4-80.6degF(18-27degC)
- C. 51.8-66.2degF(11-19degC)
- D. 44.6-60-8degF(7-16degC)

Correct Answer: B

Explanation:

The guidelines from ASHRAE establish 64.4-80.6degF (18-27degC) as the optimal temperature for a data center.

QUESTION 45

Which of the following is not a risk management framework?

- A. COBIT
- B. Hex GBL
- C. ISO 31000:2009
- D. NIST SP 800-37

Correct Answer: B

Explanation:

Hex GBL is a reference to a computer part in Terry Pratchett's fictional Discworld universe. The

rest are not.

QUESTION 46

Which of the following threat types involves the sending of untrusted data to a user's browser to be executed with their own credentials and access?

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

Correct Answer: B

Explanation:

Cross-site scripting (XSS) is an attack where a malicious actor is able to send untrusted data to a user's browser without going through any validation or sanitization processes, or where the code is not properly escaped from processing by the browser. The code is then executed on the user's browser with the user's own access and permissions, allowing an attacker to redirect their web traffic, steal data from their session, or potentially access information on the user's own computer that their browser has the ability to access.

QUESTION 47

How is an object stored within an object storage system?

- A. Key value
- B. Database
- C. LDAP
- D. Tree structure

Correct Answer: A

Explanation:

Object storage uses a flat structure with key values to store and access objects.

QUESTION 48

Which of the following is NOT a regulatory system from the United States federal government?

- A. PCI DSS
- B. FISMA
- C. SOX
- D. HIPAA

Correct Answer: A

Explanation:

The payment card industry data security standard (PCI DSS) pertains to organizations that handle credit card transactions and is an industry regulatory standard, not a governmental one.

QUESTION 49

Which jurisdiction lacks specific and comprehensive privacy laws at a national or top level of legal authority?