CCSP Q&As

Cloud Security

Pass ISC CCSP Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/ccsp.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by ISC Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which crucial aspect of cloud computing can be most threatened by insecure APIs?

A. Automation

B. Resource pooling

C. Elasticity

D. Redundancy

Correct Answer: A

Cloud environments depend heavily on API calls for management and automation. Any vulnerability with the APIs can cause significant risk and exposure to all tenants of the cloud environment. Resource pooling and elasticity could both be impacted by insecure APIs, as both require automation and orchestration to operate properly, but automation is the better answer here. Redundancy would not be directly impacted by insecure APIs.

QUESTION 2

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

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

QUESTION 3

What are SOC 1/SOC 2/SOC 3?

A. Audit reports

B. Risk management frameworks

C. Access controls

D. Software developments

Correct Answer: A

An SOC 1 is a report on controls at a service organization that may be relevant to a user entity\\'s internal control over financial reporting. An SOC 2 report is based on the existing SysTrust and WebTrust principles. The purpose of an SOC 2 report is to evaluate an organization\\'s information systems relevant to security, availability, processing integrity, confidentiality, or privacy. An SOC 3 report is also based on the existing SysTrust and WebTrust principles, like a SOC 2 report. The difference is that the SOC 3 report does not detail the testing performed.

QUESTION 4

The application normative framework is best described as which of the following?

A. A superset of the ONF

B. A stand-alone framework for storing security practices for the ONF

C. The complete ONF

D. A subnet of the ONF

Correct Answer: D

Remember, there is a one-to-many ratio of ONF to ANF; each organization has one ONF and many ANFs (one for each application in the organization). Therefore, the ANF is a subset of the ONF.

QUESTION 5

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

A. TLS

B. Testing

C. Tampering with data

D. Transport

Correct Answer: C

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 6

Which aspect of cloud computing serves as the biggest challenge to using DLP to protect data at rest?

A. Portability

B. Resource pooling

C. Interoperability

D. Reversibility

Correct Answer: B

Resource pooling serves as the biggest challenge to using DLP solutions to protect data at rest because data is spread across large systems, which are also shared by many different clients. With the data always moving and being distributed, additional challenges for protection are created versus a physical and isolated storage system. Portability is the ability to easily move between different cloud providers, and interoperability is focused on the ability to reuse components or services. Reversibility pertains to the ability of a cloud customer to easily and completely remove their data and services from a cloud provider.

QUESTION 7

Which of the following best describes SAML?

A. A standard used for directory synchronization

B. A standard for developing secure application management logistics

C. A standard for exchanging usernames and passwords across devices.

D. A standards for exchanging authentication and authorization data between security domains.

Correct Answer: D

QUESTION 8

Which of the following is considered an internal redundancy for a data center?

A. Power feeds

B. Chillers

C. Network circuits

D. Generators

Correct Answer: B

Chillers and cooling systems are internal to a data center and its operations, and as such they are considered an internal redundancy. Power feeds, network circuits, and generators are all external to a data center and provide utility services to them, which makes them an external redundancy.

QUESTION 9

Which protocol operates at the network layer and provides for full point-to-point encryption of all communications and transmissions?

A. IPSec

B. VPN

C. SSL

D. TLS

Correct Answer: A

IPSec is a protocol for encrypting and authenticating packets during transmission between two parties and can involve any type of device, application, or service. The protocol performs both the authentication and negotiation of security policies between the two parties at the start of the connection and then maintains these policies throughout the lifetime of the connection. TLS operates at the application layer, not the network layer, and is widely used to secure communications between two parties. SSL is similar to TLS but has been deprecated. Although a VPN allows a secure channel for communications into a private network from an outside location, it\\'s not a protocol.

QUESTION 10

The European Union passed the first major regulation declaring data privacy to be a human right. In what year did it go into effect?

A. 2010

B. 2000

C. 1995

D. 1990

Correct Answer: C

Adopted in 1995, Directive 95/46 EC establishes strong data protection and policy requirements, including the declaring of data privacy to be a human right. It establishes that an individual has the right to be notified when their personal data is being access or processed, that it only will ever be accessed for legitimate purposes, and that data will only be accessed to the exact extent it needs to be for the particular process or request.

QUESTION 11

Which of the following are the storage types associated with IaaS?

A. Volume and object

B. Volume and label

C. Volume and container

D. Object and target

Correct Answer: A

QUESTION 12

Which aspect of SaaS will alleviate much of the time and energy organizations spend on compliance (specifically baselines)?

A. Maintenance

B. Licensing

C. Standardization

D. Development

Correct Answer: C

With the entire software platform being controlled by the cloud provider, the standardization of configurations and versioning is done automatically for the cloud customer. This alleviates the customer\\'s need to track upgrades and releases for its own systems and development; instead, the onus is on the cloud provider. Although licensing is the responsibility of the cloud customer within SaaS, it does not have an impact on compliance requirements. Within SaaS, development and maintenance of the system are solely the responsibility of the cloud provider.

QUESTION 13

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

A. European Union

B. Germany

C. Russia

D. United States

Correct Answer: D

The United States lacks a single comprehensive law at the federal level addressing data security and privacy, but there are multiple federal laws that deal with different industries.

QUESTION 14

Which value refers to the amount of time it takes to recover operations in a BCDR situation to meet management\\'s objectives?

A. RSL

B. RPO

C. SRE

D. RTO

Correct Answer: D

The recovery time objective (RTO) is a measure of the amount of time it would take to recover operations in the event of a disaster to the point where management\\'s objectives are met for BCDR.

QUESTION 15

Which European Union directive pertains to personal data privacy and an individual\\'s control over their personal data?

A. 99/9/EC

B. 95/46/EC

C. 2000/1/EC

D. 2013/27001/EC

Correct Answer: B

Directive 95/46/EC is titled "On the protection of individuals with regard to the processing of personal data and on the free movement of such data."