



# CCSP<sup>Q&As</sup>

Cloud Security

## Pass ISC CCSP Exam with 100% Guarantee

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

<https://www.passapply.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

Where is a DLP solution generally installed when utilized for monitoring data in use?

- A. Application server
- B. Database server
- C. Network perimeter
- D. User's client

Correct Answer: D

To monitor data in use, the DLP solution's optimal location would be on the user's client or workstation, where the data would be used or processed, and where it would be most vulnerable to access or exposure. The network perimeter is most appropriate for data in transit, and an application server would serve as middle stage between data at rest and data in use, but is a less correct answer than a user's client. A database server would be an example of a location appropriate for monitoring data at rest.

---

### QUESTION 2

All the following are data analytics modes, except: A. Datamining

- B. Agile business intelligence
- C. Refractory iterations
- D. Real-time analytics

Correct Answer: C

All the others are data analytics methods, but "refractory iterations" is a nonsense term thrown in as a red herring.

---

### QUESTION 3

Which technology can be useful during the "share" phase of the cloud data lifecycle to continue to protect data as it leaves the original system and security controls?

- A. IPS
- B. WAF
- C. DLP
- D. IDS

Correct Answer: C

Data loss prevention (DLP) can be applied to data that is leaving the security enclave to continue to enforce access restrictions and policies on other clients and systems.

---



#### QUESTION 4

Which data protection strategy would be useful for a situation where the ability to remove sensitive data from a set is needed, but a requirement to retain the ability to map back to the original values is also present?

- A. Masking
- B. Tokenization
- C. Encryption
- D. Anonymization

Correct Answer: B

Tokenization involves the replacement of sensitive data fields with key or token values, which can ultimately be mapped back to the original, sensitive data values. Masking refers to the overall approach to covering sensitive data, and anonymization is a type of masking, where indirect identifiers are removed from a data set to prevent the mapping back of data to an individual. Encryption refers to the overall process of protecting data via key pairs and protecting confidentiality.

---

#### QUESTION 5

Which of the following threat types can occur when baselines are not appropriately applied or unauthorized changes are made?

- A. Insecure direct object references
- B. Unvalidated redirects and forwards
- C. Security misconfiguration
- D. Sensitive data exposure

Correct Answer: C

Security misconfigurations occur when applications and systems are not properly configured or maintained in a secure manner. This can be caused from a shortcoming in security baselines or configurations, unauthorized changes to system configurations, or a failure to patch and upgrade systems as the vendor releases security patches.

---

#### QUESTION 6

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 7

In addition to whatever audit results the provider shares with the customer, what other mechanism does the customer have to ensure trust in the provider's performance and duties?

- A. HIPAA
- B. The contract
- C. Statutes
- D. Security control matrix

Correct Answer: B

The contract between the provider and customer enhances the customer's trust by holding the provider financially liable for negligence or inadequate service (although the customer remains legally liable for all inadvertent disclosures). Statutes, however, largely leave customers liable. The security control matrix is a tool for ensuring compliance with regulations. HIPAA is a statute.

---

#### QUESTION 8

Upon completing a risk analysis, a company has four different approaches to addressing risk. Which approach it takes will be based on costs, available options, and adherence to any regulatory requirements from independent audits.

Which of the following groupings correctly represents the four possible approaches?

- A. Accept, avoid, transfer, mitigate
- B. Accept, deny, transfer, mitigate
- C. Accept, deny, mitigate, revise
- D. Accept, dismiss, transfer, mitigate

Correct Answer: A

The four possible approaches to risk are as follows: accept (do not patch and continue with the risk), avoid (implement solutions to prevent the risk from occurring), transfer (take out insurance), and mitigate (change configurations or patch to resolve the risk). Each of these answers contains at least one incorrect approach name.

---

#### QUESTION 9



Which of the following would be considered an example of insufficient due diligence leading to security or operational problems when moving to a cloud?

- A. Monitoring
- B. Use of a remote key management system
- C. Programming languages used
- D. Reliance on physical network controls

Correct Answer: D

Many organizations in a traditional data center make heavy use of physical network controls for security. Although this is a perfectly acceptable best practice in a traditional data center, this reliance is not something that will port to a cloud environment. The failure of an organization to properly understand and adapt to the difference in network controls when moving to a cloud will likely leave an application with security holes and vulnerabilities. The use of a remote key management system, monitoring, or certain programming languages would not constitute insufficient due diligence by itself.

---

#### QUESTION 10

What is the biggest benefit to leasing space in a data center versus building or maintain your own?

- A. Certification
- B. Costs
- C. Regulation
- D. Control

Correct Answer: B

When leasing space in a data center, an organization can avoid the enormous startup and building costs associated with a data center, and can instead leverage economies of scale by grouping with other organizations and sharing costs.

---

#### QUESTION 11

Which of the following would make it more likely that a cloud provider would be unwilling to satisfy specific certification requirements?

- A. Resource pooling
- B. Virtualization
- C. Multitenancy
- D. Regulation

Correct Answer: C



With cloud providers hosting a number of different customers, it would be impractical for them to pursue additional certifications based on the needs of a specific customer. Cloud environments are built to a common denominator to serve the greatest number of customers, and especially within a public cloud model, it is not possible or practical for a cloud provider to alter their services for specific customer demands.

---

#### QUESTION 12

Although the United States does not have a single, comprehensive privacy and regulatory framework, a number of specific regulations pertain to types of data or populations.

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

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

Correct Answer: D

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. The Sarbanes-Oxley Act (SOX) was passed in 2002 and pertains to financial records and reporting, as well as transparency requirements for shareholders and other stakeholders. The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 and pertains to data privacy and security for medical records. FISMA refers to the Federal Information Security Management Act of 2002 and pertains to the protection of all US federal government IT systems, with the exception of national security systems.

---

#### QUESTION 13

Which of the following are attributes of cloud computing?

- A. Minimal management effort and shared resources
- B. High cost and unique resources
- C. Rapid provisioning and slow release of resources
- D. Limited access and service provider interaction

Correct Answer: A

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

---

#### QUESTION 14

What are third-party providers of IAM functions for the cloud environment?



- A. AESs
- B. SIEMs
- C. DLPs
- D. CASBs

Correct Answer: D

Data loss, leak prevention, and protection is a family of tools used to reduce the possibility of unauthorized disclosure of sensitive information. SIEMs are tools used to collate and manage log data. AES is an encryption standard.

---

#### QUESTION 15

Best practices for key management include all of the following, except:

- A. Ensure multifactor authentication
- B. Pass keys out of band
- C. Have key recovery processes
- D. Maintain key security

Correct Answer: A

We should do all of these except for requiring multifactor authentication, which is pointless in key management.

[Latest CCSP Dumps](#)

[CCSP PDF Dumps](#)

[CCSP Practice Test](#)