

CCSP^{Q&As}

Cloud Security

Pass ISC CCSP Exam with 100% Guarantee

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

<https://www.leads4pass.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 ITIL component is focused on anticipating predictable problems and ensuring that configurations and operations are in place to prevent these problems from ever occurring?

- A. Availability management
- B. Continuity management
- C. Configuration management
- D. Problem management

Correct Answer: D

Problem management is focused on identifying and mitigating known problems and deficiencies before they are able to occur, as well as on minimizing the impact of incidents that cannot be prevented. Continuity management (or business continuity management) is focused on planning for the successful restoration of systems or services after an unexpected outage, incident, or disaster. Availability management is focused on making sure system resources, processes, personnel, and toolsets are properly allocated and secured to meet SLA requirements. Configuration management tracks and maintains detailed information about all IT components within an organization.

QUESTION 2

Which of the following threat types involves the sending of commands or arbitrary data through input fields in an application in an attempt to get that code executed as part of normal processing?

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

Correct Answer: C

An injection attack is where a malicious actor will send commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries. This can trick an application into exposing data that is not intended or authorized to be exposed, or it could potentially allow an attacker to gain insight into configurations or security controls. Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call. Cross-site request forgery occurs when an attack forces an authenticated user to send forged requests to an application running under their own access and credentials. Cross-site scripting occurs when an attacker is able to send untrusted data to a user's browser without going through validation processes.

QUESTION 3

You just hired an outside developer to modernize some applications with new web services and functionality. In order to implement a comprehensive test platform for validation, the developer needs a

data set that resembles a production data set in both size and composition.

In order to accomplish this, what type of masking would you use?

- A. Development
- B. Replicated
- C. Static
- D. Dynamic

Correct Answer: C

Static masking takes a data set and produces a copy of it, but with sensitive data fields masked. This allows for a full data set from production for testing purposes, but without any sensitive data. Dynamic masking works with a live system and is not used to produce a distinct copy. The terms "replicated" and "development" are not types of masking.

QUESTION 4

Which of the following threat types involves leveraging a user's browser to send untrusted data to be executed with legitimate access via the user's valid credentials?

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

Correct Answer: D

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 perhaps the code is not properly escaped from processing by the browser. The code is then executed on the user's browser with their own access and permissions, allowing the attacker to redirect the user's 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. Missing function-level access control exists where an application only checks for authorization during the initial login process and does not further validate with each function call. An injection attack is where a malicious actor sends commands or other arbitrary data through input and data fields with the intent of having the application or system execute the code as part of its normal processing and queries. Cross-site request forgery occurs when an attack forces an authenticated user to send forged requests to an application running under their own access and credentials.

QUESTION 5

A localized incident or disaster can be addressed in a cost-effective manner by using which of the following?

- A. UPS
- B. Generators
- C. Joint operating agreements

D. Strict adherence to applicable regulations

Correct Answer: C

Joint operating agreements can provide nearby relocation sites so that a disruption limited to the organization's own facility and campus can be addressed at a different facility and campus. UPS and generators are not limited to serving needs for localized causes. Regulations do not promote cost savings and are not often the immediate concern during BC/DR activities.

[CCSP Practice Test](#)

[CCSP Study Guide](#)

[CCSP Exam Questions](#)