CSSLP[Q&As]

Certified Secure Software Lifecycle Professional Practice Test

Pass ISC CSSLP Exam with 100% Guarantee

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

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

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You are responsible for network and information security at a metropolitan police station. The most important concern is that unauthorized parties are not able to access data. What is this called?

A. Confidentiality

B. Availability

C. Integrity

D. Encryption

Correct Answer: A

The CIA (Confidentiality, Integrity, and Availability) triangle is concerned with three facets of security. Confidentiality is the concern that data be secure from unauthorized access. Answer: B and C are incorrect. The CIA (Confidentiality, Integrity, and Availability) triangle is concerned with three facets of security. Integrity is the concern that data not be altered without it being traceable. Availability is the concern that the data, while being secured, is readily accessible. Answer: D is incorrect. Confidentiality may be implemented with encryption but encryption is just a technique to obtain confidentiality.

QUESTION 2

Which of the following plans is designed to protect critical business processes from natural or man-made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes?

A. Contingency plan

B. Business continuity plan

C. Crisis communication plan

D. Disaster recovery plan

Correct Answer: B

The business continuity plan is designed to protect critical business processes from natural or man-made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan. Answer: C is incorrect. The crisis communication plan can be broadly defined as the plan for the exchange of information before, during, or after a crisis event. It is considered as a sub-specialty of the public relations profession that is designed to protect and defend an individual, company, or organization facing a public challenge to its reputation. The aim of crisis communication plan is to assist organizations to achieve continuity of critical business processes and information flows under crisis, disaster or event driven circumstances. Answer: A is incorrect. A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and "triggers" for initiating planned actions. They are required to help governments, businesses, or individuals to recover

from serious incidents in the minimum time with minimum cost and disruption. Answer: D is incorrect. A disaster recovery plan should contain data, hardware, and software that can be critical for a business. It should also include the plan for sudden loss such as hard disc crash. The business should use backup and data recovery utilities to limit the loss of data.

QUESTION 3

Which of the following classification levels defines the information that, if disclosed to the unauthorized parties, could be reasonably expected to cause exceptionally grave damage to the national security?

A. Secret information

B. Unclassified information

C. Confidential information

D. Top Secret information

Correct Answer: D

Top Secret information is the highest level of classification of material on a national level. Such material would cause "exceptionally grave damage" to national security if publicly available. Answer: A is incorrect. Secret information is that, if disclosed to unauthorized parties, could be expected to cause serious damage to the national security, but it is not the best answer for the above question. Answer: C is incorrect. Such material would cause "damage" or be "prejudicial" to national security if publicly available. Answer: B is incorrect. Unclassified information, technically, is not a classification level, but is used for government documents that do not have a classification listed above. Such documents can sometimes be viewed by those without security clearance.

QUESTION 4

An authentication method uses smart cards as well as usernames and passwords for authentication. Which of the following authentication methods is being referred to?

A. Anonymous

B. Mutual

C. Multi-factor

D. Biometrics

Correct Answer: C

Multi-factor authentication involves a combination of multiple methods of authentication. For example, an authentication method that uses smart cards as well as usernames and passwords can be referred to as multi-factor authentication. Answer: B is incorrect. Mutual authentication is a process in which a client process and server are required to prove their identities to each other before performing any application function. The client and server identities can be verified through a trusted third party and use shared secrets as in the case of Kerberos v5. The MS-CHAP v2 and EAP-TLS authentication methods support mutual authentication. Answer: A is incorrect. Anonymous authentication is an authentication method used for Internet communication. It provides limited access to specific public folders and directory information. It is supported by all clients and is used to access unsecured content in public folders. An administrator must create a user account in IIS to enable the user to connect anonymously. Answer: D is incorrect. Biometrics authentication uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical

qualities to identify a user.

QUESTION 5

You work as a Security Manager for Tech Perfect Inc. The company has a Windows based network. It is required to determine compatibility of the systems with custom applications. Which of the following techniques will you use to accomplish the task?

A. Safe software storage

B. Antivirus management

C. Backup control

D. Software testing

Correct Answer: D

In order to accomplish the task, you should use the software testing technique. By using this technique you can determine compatibility of systems with custom applications or you can identify other unforeseen interactions. You can also use the software testing technique whileyou are upgrading software. Answer: B is incorrect. You can use the antivirus management to save the systems from viruses, unexpected software interactions, and the subversion of security controls. Answer: A is incorrect. You can use the safe software storage technique to ensure that the software and backup copies have not been modified without authorization. Answer: C is incorrect. You can use the backup control to perform back up of software and data.