# 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.passapply.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**

Mark works as a Network Administrator for NetTech Inc. He wants users to access only those resources that are required for them. Which of the following access control models will he use?

A. Discretionary Access Control

B. Mandatory Access Control

C. Policy Access Control

D. Role-Based Access Control

Correct Answer: D

Role-based access control (RBAC) is an access control model. In this model, a user can access resources according to his role in the organization. For example, a backup administrator is responsible for taking backups of important data. Therefore, he is only authorized to access this data for backing it up. However, sometimes users with different roles need to access the same resources. This situation can also be handled using the RBAC model. Answer: B is incorrect. Mandatory Access Control (MAC) is a model that uses a predefined set of access privileges for an object of the system. Access to an object is restricted on the basis of the sensitivity of the object and granted through authorization. Sensitivity of an object is defined by the label assigned to it. For example, if a user receives a copy of an object that is marked as "secret", he cannot grant permission to other users to see this object unless they have the appropriate permission. Answer: A is incorrect. DAC is an access control model. In this model, the data owner has the right to decide who can access the data. This model is commonly used in PC environment. The basis of this model is the use of Access Control List (ACL). Answer: C is incorrect. There is no such access control model as Policy Access Control.

**QUESTION 2**

Which of the following is a chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event?

A. Corrective controls

B. Audit trail

C. Security audit

D. Detective controls

Correct Answer: B

Audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function. Audit records typically result from activities such as transactions or communications by individual people, systems, accounts, or other entities. The process that creates audit trail should always run in a privileged mode, so it could access and supervise all actions from all users, and normal user could not stop/change it. Furthermore, for the same reason, trail file or database table with a trail should not be accessible to normal users. Answer: C is incorrect. A computer security audit is a manual or systematic measurable technical assessment of a system or application. Manual assessments include interviewing staff, performing security vulnerability scans, reviewing application and operating system access controls, and analyzing physical access to the systems. Automated assessments, or CAAT\\'s, include system generated audit reports or using software to monitor and report changes to files and settings on a system. Systems can include personal computers, servers, mainframes, network routers, and switches. Answer: D is incorrect. Detective controls are the audit controls that are not

needed to be restricted. Any control that performs a monitoring activity can likely be defined as a Detective Control. For example, it is possible that mistakes, either intentional or unintentional, can be made. Therefore, an additional Protective control is that these companies must have their financial results audited by an independent Certified Public Accountant. The role of this accountant is to act as an auditor. In fact, any auditor acts as a Detective control. If the organization in question has not properly followed the rules, a diligent auditor should be able to detect the deficiency which indicates that some control somewhere has failed. Answer: A is incorrect. Reactive or corrective controls typically work in response to a detective control, responding in such a way as to alert or otherwise correct an unacceptable condition. Using the example of account rules, either the internal Audit Committee or the SEC itself, based on the report generated by the external auditor, will take some corrective action. In this way, they are acting as a Corrective or Reactive control.

**QUESTION 3**

Which of the following DITSCAP phases validates that the preceding work has produced an IS that operates in a specified computing environment?

A. Phase 2

B. Phase 4

C. Phase 1

D. Phase 3

Correct Answer: D

The Phase 3 of DITSCAP CandA is known as Validation. The goal of Phase 3 is to validate that the preceding work has produced an IS that operates in a specified computing environment. Answer: C is incorrect. The goal of this phase is to define the CandA level of effort, identify the main CandA roles and responsibilities, and create an agreement on the method for implementing the security requirements. Answer: A is incorrect. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. Answer: B is incorrect. This phase ensures that it will maintain an acceptable level of residual risk.

**QUESTION 4**

How can you calculate the Annualized Loss Expectancy (ALE) that may occur due to a threat?

A. Single Loss Expectancy (SLE) X Annualized Rate of Occurrence (ARO)

B. Single Loss Expectancy (SLE)/ Exposure Factor (EF)

C. Asset Value X Exposure Factor (EF)

D. Exposure Factor (EF)/Single Loss Expectancy (SLE)

Correct Answer: A

The Annualized Loss Expectancy (ALE) that occurs due to a threat can be calculated by multiplying the Single Loss Expectancy (SLE) with the Annualized Rate of Occurrence (ARO). Annualized Loss Expectancy (ALE) = Single Loss Expectancy (SLE) X Annualized Rate of Occurrence (ARO) Annualized Rate of Occurrence (ARO) is a number that represents the estimated frequency in which a threat is expected to occur. It is calculated based upon the probability of the event occurring and the number of employees that could make that event occur. Single Loss Expectancy (SLE) is the value in dollars that is assigned to a single event. SLE can be calculated by the following formula: SLE = Asset Value ($) X Exposure Factor (EF) The Exposure Factor (EF) represents the % of assets loss caused by a threat. The

EF is required to calculate Single Loss Expectancy (SLE).

**QUESTION 5**

Which of the following terms refers to a mechanism which proves that the sender really sent a particular message?

A. Confidentiality

B. Non-repudiation

C. Authentication

D. Integrity

Correct Answer: B

Non-repudiation is a mechanism which proves that the sender really sent a message. It provides an evidence of the identity of the senderand message integrity. It also prevents a person from denying the submission or delivery of the message and the integrity of its contents. Answer: C is incorrect. Authentication is a process of verifying the identity of a person or network host. Answer: A is incorrect. Confidentiality ensures that no one can read a message except the intended receiver. Answer: D is incorrect. Integrity assures the receiver that the received message has not been altered in any way from the original.

**QUESTION 6**

In which of the following levels of exception safety are operations succeeded with full guarantee and fulfill all needs in the presence of exceptional situations?

A. Commit or rollback semantics

B. Minimal exception safety

C. Failure transparency

D. Basic exception safety

Correct Answer: C

Failure transparency is the best level of exception safety. In this level, operations are succeeded with full guarantee and fulfill all needs in the presence of exceptional situations. Failure transparency does not throw the exception further up even when an exception occurs. This level is also known as no throw guarantee.

**QUESTION 7**

The build environment of secure coding consists of some tools that actively support secure specification, design, and implementation. Which of the following features do these tools have? Each correct answer represents a complete solution. Choose all that apply.

A. They decrease the exploitable flaws and weaknesses.

B. They reduce and restrain the propagation, extent, and damage that have occurred by insecure software behavior.

C. They decrease the attack surface.

D. They employ software security constraints, protections, and services. E. They decrease the level of type checking and program analysis.

Correct Answer: ABCD

The tools that produce secure software have the following features: They decrease the exploitable flaws and weaknesses. They decrease the attack surface. They employ software security constraints, protections, and services. They reduce and restrain the propagation, extent, and damage that are caused by the behavior of insecure software. Answer: E is incorrect. This feature is not required for these tools.

**QUESTION 8**

Which of the following are the primary functions of configuration management?

Each correct answer represents a complete solution. Choose all that apply.

A. It removes the risk event entirely by adding additional steps to avoid the event.

B. It ensures that the change is implemented in a sequential manner through formalized testing.

C. It reduces the negative impact that the change might have had on the computing services and resources.

D. It analyzes the effect of the change that is implemented on the system.

Correct Answer: BCD

The primary functions of configuration management are as follows: It ensures that the change is implemented in a sequential manner through formalized testing. It ensures that the user base is informed of the future change. It analyzes the effect of the change that is implemented on the system. It reduces the negative impact that the change might have had on the computing services and resources. Answer: A is incorrect. It is not one of the primary functions of configuration management. It is the function of risk avoidance.

**QUESTION 9**

Stella works as a system engineer for BlueWell Inc. She wants to identify the performance thresholds of each build. Which of the following tests will help Stella to achieve her task?

A. Reliability test

B. Performance test

C. Regression test

D. Functional test

Correct Answer: B

The various types of internal tests performed on builds are as follows: Regression tests: It is also known as the verification testing. These tests are developed to confirm that capabilities in earlier builds continue to work correctly in the

subsequent builds. Functional test:

These tests emphasizes on verifying that the build meets its functional and data requirements and correctly generates each expected display and report. Performance tests: These tests are used to identify the performance thresholds of each

build. Reliability tests: These tests are used to identify the reliability thresholds of each build.

**QUESTION 10**

Della works as a security engineer for BlueWell Inc. She wants to establish configuration management and control procedures that will document proposed or actual changes to the information system. Which of the following phases of NIST SP 800-37 CandA methodology will define the above task?

A. Initiation

B. Security Certification

C. Continuous Monitoring

D. Security Accreditation

Correct Answer: C

The various phases of NIST SP 800-37 CandA are as follows:

Phase 1: Initiation- This phase includes preparation, notification and resource identification. It performs the security plan analysis, update, and acceptance. Phase 2: Security Certification- The Security certification phase evaluates the controls

and documentation. Phase 3: Security Accreditation- The security accreditation phase examines the residual risk for acceptability, and prepares the final security accreditation package. Phase 4: Continuous Monitoring-This phase monitors

the configuration management and control, ongoing security control verification, and status reporting and documentation.

**QUESTION 11**

The service-oriented modeling framework (SOMF) provides a common modeling notation to address alignment between business and IT organizations. Which of the following principles does the SOMF concentrate on? Each correct answer represents a part of the solution. Choose all that apply.

A. Architectural components abstraction

B. SOA value proposition

C. Business traceability

D. Disaster recovery planning

E. Software assets reuse

Correct Answer: ABCE

The service-oriented modeling framework (SOMF) concentrates on the following principles:

Business traceability Architectural best-practices traceability Technological traceability SOA value proposition Software assets reuse SOA integration strategies Technological abstraction and generalization Architectural components

abstraction Answer: D is incorrect. The service- oriented modeling framework (SOMF) does not concentrate on it.

**QUESTION 12**

What are the various benefits of a software interface according to the "Enhancing the Development Life Cycle to Produce Secure Software" document? Each correct answer represents a complete solution. Choose three.

A. It modifies the implementation of a component without affecting the specifications of the interface.

B. It controls the accessing of a component.

C. It displays the implementation details of a component.

D. It provides a programmatic way of communication between the components that are working with different programming languages.

Correct Answer: ABD

The benefits of a software interface are as follows: It provides a programmatic way of communication between the components that are working with different programming languages. It prevents direct communication between components. It modifies the implementation of a component without affecting the specifications of the interface. It hides the implementation details of a component. It controls the accessing of a component. Answer: C is incorrect. A software interface hides the implementation details of the component.

**QUESTION 13**

Samantha works as an Ethical Hacker for we-are-secure Inc. She wants to test the security of the we-are-secure server for DoS attacks. She sends large number of ICMP ECHO packets to the target computer. Which of the following DoS attacking techniques will she use to accomplish the task?

A. Smurf dos attack

B. Land attack

C. Ping flood attack

D. Teardrop attack

Correct Answer: C

According to the scenario, Samantha is using the ping flood attack. In a ping flood attack, an attacker sends a large number of ICMP packets to the target computer using the ping command, i.e., ping -f target_IP_address. When the target computer receives these packets in large quantities, it does not respond and hangs. However, for such an attack to take place, the attacker must have sufficient Internet bandwidth, because if the target responds with an "ECHO reply ICMP packet" message, the attacker must have both the incoming and outgoing bandwidths available for communication. Answer: A is incorrect. In a smurf DoS attack, an attacker sends a large amount of ICMP echo request

traffic to the IP broadcast addresses. These ICMP requests have a spoofed source address of the intended victim. If the routing device delivering traffic to those broadcast addresses delivers the IP broadcast to all the hosts, most of the IP addresses send an ECHO reply message. However, on a multi- access broadcast network, hundreds of computers might reply to each packet when the target network is overwhelmed by all the messages sent simultaneously. Due to this, the network becomes unable to provide services to all the messages and crashes. Answer: D is incorrect. In a teardrop attack, a series of data packets are sent to the target computer with overlapping offset field values. As a result, the target computer is unable to reassemble these packets and is forced to crash, hang, or reboot. Answer: B is incorrect. In a land attack, the attacker sends a spoofed TCP SYN packet in which the IP address of the target is filled in both the source and destination fields. On receiving the spoofed packet, the target system becomes confused and goes into a frozen state. Now-a-days, antivirus can easily detect such an attack.

**QUESTION 14**

Which of the following phases of the DITSCAP CandA process is used to define the CandA level of effort, to identify the main CandA roles and responsibilities, and to create an agreement on the method for implementing the security requirements?

A. Phase 1

B. Phase 4

C. Phase 2

D. Phase 3

Correct Answer: A

The Phase 1 of the DITSCAP CandA process is known as Definition Phase. The goal of this phase is to define the CandA level of effort, identify the main CandA roles and responsibilities, and create an agreement on the method for implementing the security requirements. Answer: C is incorrect. The Phase 2 of the DITSCAP CandA process is known as Verification. Answer: D is incorrect. The Phase 3 of the DITSCAP CandA process is known as Validation. Answer: B is incorrect. The Phase 4 of the DITSCAP CandA process is known as Post Accreditation.

**QUESTION 15**

Which of the following are the types of intellectual property? Each correct answer represents a complete solution. Choose all that apply.

A. Patent

B. Copyright

C. Standard

D. Trademark

Correct Answer: AB

Common types of intellectual property include copyrights, trademarks, patents, industrial design rights, and trade secrets. A copyright is a form of intellectual property, which secures to its holder the exclusive right to produce copies of his or her works of original expression, such as a literary work, movie, musical work or sound recording, painting, photograph, computer program, or industrial design, for a defined, yet extendable, period of time. It does not cover ideas or facts. Copyright laws protect intellectual property from misuse by other individuals. A trademark is a distinctive sign

used by an individual, business organization, or other legal entity to identify that the products or services to consumers with which the trademark appears originate from a unique source, and to distinguish its products or services from those of other entities. A trademark is designated by the following symbols: : It is for an unregistered trade mark and it is used to promote or brand goods. : It is for an unregistered service mark and it is used to promote or brand services. : It is for a registered trademark. A patent is a set of exclusive rights granted by a state to an inventor or their assignee for a limited period of time in exchange for a public disclosure of an invention. Answer: C is incorrect. It is not a type of intellectual property.