

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

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



QUESTION 1

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 2

Which of the following is used by attackers to record everything a person types, including usernames, passwords, and account information?

- A. Packet sniffing
- B. Keystroke logging
- C. Spoofing
- D. Wiretapping

Correct Answer: B

Keystroke logging is used by attackers to record everything a person types, including usernames, passwords, and account information. Keystroke logging is a method of logging and recording user keystrokes. It can be performed with software or hardware devices. Keystroke logging devices can record everything a person types using his keyboard, such as to measure employee's productivity on certain clerical tasks. These types of devices can also be used to get usernames, passwords, etc. Answer: D is incorrect. Wiretapping is used to eavesdrop on voice calls. Eavesdropping is the process of listening in on private conversations. It also includes attackers listening in on network traffic. Answer: C is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected. Answer: A is incorrect. Packet sniffing is a process of monitoring data packets that travel across a network. The software used for packet sniffing is known as sniffers. There are many packet-sniffing programs that are available on the Internet. Some of these are unauthorized, which can be harmful for a network's security.

QUESTION 3

Which of the following programming languages are compiled into machine code and directly executed by the CPU of a computer system? Each correct answer represents a complete solution. Choose two.

- A. C
- B. Microosft.NET
- C. Java EE
- D. C++

Correct Answer: AD

C and C++ programming languages are unmanaged code. Unmanaged code is compiled into machine code and directly executed by the CPU of a computer system. Answer: C and B are incorrect. Java EE and Microsoft.Net are compiled into an intermediate code format.

QUESTION 4

Which of the following is a variant with regard to Configuration Management?

- A. A CI that has the same name as another CI but shares no relationship.
- B. A CI that particularly refers to a software version.
- C. A CI that has the same essential functionality as another CI but a bit different in some small manner.
- D. A CI that particularly refers to a hardware specification.

Correct Answer: C

A CI that has the same essential functionality as another CI but a bit different in some small manner, and therefore, might be required to be analyzed along with its generic group. A Configuration item (CI) is an IT asset or a combination of IT assets that may depend and have relationships with other IT processes. A CI will have attributes which may be hierarchical and relationships that will be assigned by the configuration manager in the CM database. The Configuration Item (CI) attributes are as follows: 1. Technical: It is data that describes the CI's capabilities which include software version and model numbers, hardware and manufacturer specifications, and other technical details like networking speeds, and data storage size. Keyboards, mice and cables are considered consumables. 2. Ownership: It is part of financial asset management, ownership attributes, warranty, location, and responsible person for the CI. 3. Relationship: It is the relationship among hardware items, software, and users. Answer: B, D, and A are incorrect. These are incorrect definitions of a variant with regard to Configuration Management.

QUESTION 5

The LeGrand Vulnerability-Oriented Risk Management method is based on vulnerability analysis and consists of four principle steps. Which of the following processes does the risk assessment step include? Each correct answer represents a part of the solution. Choose all that apply.

- A. Remediation of a particular vulnerability

- B. Cost-benefit examination of countermeasures
- C. Identification of vulnerabilities
- D. Assessment of attacks

Correct Answer: BCD

Risk assessment includes identification of vulnerabilities, assessment of losses caused by threats materialized, cost-benefit examination of countermeasures, and assessment of attacks. Answer: A is incorrect. This process is included in the vulnerability management.

QUESTION 6

Which of the following security models characterizes the rights of each subject with respect to every object in the computer system?

- A. Clark-Wilson model
- B. Bell-LaPadula model
- C. Biba model
- D. Access matrix

Correct Answer: D

The access matrix or access control matrix is an abstract, formal security model of protection state in computer systems that characterizes the rights of each subject with respect to every object in the system. It was first introduced by Butler W. Lampson in 1971. According to the access matrix model, the protection state of a computer system can be abstracted as a set of objects $\{O\}$, that is the set of entities that needs to be protected (e.g. processes, files, memory pages) and a set of subjects $\{S\}$ that consists of all active entities (e.g. users, processes). Further there exists a set of rights $\{R\}$ of the form $r(s,o)$, where $s \in S$, $o \in O$ and $r(s,o) \in R$. A right thereby specifies the kind of access a subject is allowed to process with regard to an object. Answer: B is incorrect. The Bell-La Padula Model is a state machine model used for enforcing access control in government and military applications. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g., "Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public"). The Bell-La Padula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity. Answer: A is incorrect. The Clark- Wilson model provides a foundation for specifying and analyzing an integrity policy for a computing system. The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. The model's enforcement and certification rules define data items and processes that provide the basis for an integrity policy. The core of the model is based on the notion of a transaction. Answer: C is incorrect. The Biba model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject.

QUESTION 7

Which of the following acts is used to recognize the importance of information security to the economic and national security interests of the United States?

- A. Computer Misuse Act
- B. Lanham Act
- C. Computer Fraud and Abuse Act
- D. FISMA

Correct Answer: D

The Federal Information Security Management Act of 2002 is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002. The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA has brought attention within the federal government to cybersecurity and explicitly emphasized a risk-based policy for cost-effective security. FISMA requires agency program officials, chief information officers, and Inspectors General (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget (OMB). OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act. Answer: B is incorrect. The Lanham Act is a piece of legislation that contains the federal statutes of trademark law in the United States. The Act prohibits a number of activities, including trademark infringement, trademark dilution, and false advertising. It is also called Lanham Trademark Act. Answer: A is incorrect. The Computer Misuse Act 1990 is an act of the UK Parliament which states the following statement: Unauthorized access to the computer material is punishable by 6 months imprisonment or a fine "not exceeding level 5 on the standard scale" (currently 5000). Unauthorized access with the intent to commit or facilitate commission of further offences is punishable by 6 months/maximum fine on summary conviction or 5 years/fine on indictment. Unauthorized modification of computer material is subject to the same sentences as section 2 offences. Answer: C is incorrect. The Computer Fraud and Abuse Act is a law passed by the United States Congress in 1984 intended to reduce cracking of computer systems and to address federal computer-related offenses. The Computer Fraud and Abuse Act (codified as 18 U.S.C. 1030) governs cases with a compelling federal interest, where computers of the federal government or certain financial institutions are involved, where the crime itself is interstate in nature, or computers used in interstate and foreign commerce. It was amended in 1986, 1994, 1996, in 2001 by the USA PATRIOT Act, and in 2008 by the Identity Theft Enforcement and Restitution Act. Section (b) of the act punishes anyone who not just commits or attempts to commit an offense under the Computer Fraud and Abuse Act but also those who conspire to do so.

QUESTION 8

Software Development Life Cycle (SDLC) is a logical process used by programmers to develop software. Which of the following SDLC phases meets the audit objectives defined below: System and data are validated. System meets all user requirements. System meets all control requirements.

- A. Evaluation and acceptance
- B. Programming and training
- C. Definition
- D. Initiation

Correct Answer: A

It is the evaluation and acceptance phase of the SDLC, which meets the following audit objectives: System and data are validated. System meets all user requirements. System meets all control requirements Answer: D is incorrect. During the initiation phase, the need for a system is expressed and the purpose of the system is documented. Answer: C is

incorrect. During the definition phase, users\' needs are defined and the needs are translated into requirements statements that incorporate appropriate controls. Answer: B is incorrect. During the programming and training phase, the software and other components of the system are faithfully incorporated into the design specifications. Proper documentation and training are provided in this phase.

QUESTION 9

Which of the following security issues does the Bell-La Padula model focus on?

- A. Authorization
- B. Confidentiality
- C. Integrity
- D. Authentication

Correct Answer: B

The Bell-La Padula model is a state machine model used for enforcing access control in large organizations. It focuses on data confidentiality and access to classified information, in contrast to the Biba Integrity model, which describes rules for the protection of data integrity. In the Bell-La Padula model, the entities in an information system are divided into subjects and objects. The Bell-La Padula model is built on the concept of a state machine with a set of allowable states in a computer network system. The transition from one state to another state is defined by transition functions. The model defines two mandatory access control (MAC) rules and one discretionary access control (DAC) rule with three security properties: 1.The Simple Security Property: A subject at a given security level may not read an object at a higher security level (no read-up). 2.The *-property (star-property): A subject at a given security level must not write to any object at a lower security level (no write-down). The *-property is also known as the Confinement property. 3.The Discretionary Security Property: It uses an access matrix to specify the discretionary access control.

QUESTION 10

Which of the following governance bodies provides management, operational and technical controls to satisfy security requirements?

- A. Senior Management
- B. Business Unit Manager
- C. Information Security Steering Committee
- D. Chief Information Security Officer

Correct Answer: A

Senior management provides management, operational and technical controls to satisfy security requirements. The governance roles and responsibilities are mentioned below in the table:

Governance Body	Membership	Responsibilities
Information Security Steering Committee	CFO, CEO, COO, CTO, VP Business units chaired by CISO	It establishes and supports security programs
Senior Management	C-level, unit VPs and senior VPs	It provides management, operational and technical controls to satisfy security requirements.
Chief Information Security Officer	CISO and staff	It directs and coordinates implementations of information security program.
Business Unit Managers	Department heads and supervisors	They Classify and establish requirements for safeguarding information assets.

QUESTION 11

Information Security management is a process of defining the security controls in order to protect information assets. The first action of a management program to implement information security is to have a security program in place. What are the objectives of a security program? Each correct answer represents a complete solution. Choose all that apply.

- A. Security education
- B. Security organization
- C. System classification
- D. Information classification

Correct Answer: ABD

The first action of a management program to implement information security is to have a security program in place. The objectives of a security program are as follows: Protect the company and its assets Manage risks by identifying assets, discovering threats, and estimating the risk Provide direction for security activities by framing of information security policies, procedures, standards, guidelines and baselines Information classification Security organization Security education Answer: C is incorrect. System classification is not one of the objectives of a security program.

QUESTION 12

There are seven risks responses that a project manager can choose from. Which risk response is appropriate for both positive and negative risk events?

- A. Acceptance
- B. Transference
- C. Sharing
- D. Mitigation

Correct Answer: A

Only acceptance is appropriate for both positive and negative risk events. Often sharing is used for low probability and low impact risk events regardless of the positive or negative effects the risk event may bring the project. Acceptance response is a part of Risk Response planning process. Acceptance response delineates that the project plan will not be changed to deal with the risk. Management may develop a contingency plan if the risk does occur. Acceptance response to a risk event is a strategy that can be used for risks that pose either threats or opportunities. Acceptance response can be of two types: Passive acceptance: It is a strategy in which no plans are made to try or avoid or mitigate the risk. Active acceptance: Such responses include developing contingency reserves to deal with risks, in case they occur. Acceptance is the only response for both threats and opportunities. Answer: C is incorrect. Sharing is a positive risk response that shares an opportunity for all parties involved in the risk event. Answer: B is incorrect. Transference is a negative risk event that transfers the risk ownership to a third party, such as vendor, through a contractual relationship. Answer: D is incorrect. Mitigation is a negative risk event that seeks to lower the probability and/or impact of a risk event.

QUESTION 13

You work as the Senior Project manager in Dotcoiss Inc. Your company has started a software project using configuration management and has completed 70% of it. You need to ensure that the network infrastructure devices and networking standards used in this project are installed in accordance with the requirements of its detailed project design documentation. Which of the following procedures will you employ to accomplish the task?

- A. Configuration identification
- B. Configuration control
- C. Functional configuration audit
- D. Physical configuration audit

Correct Answer: D

Physical Configuration Audit (PCA) is one of the practices used in Software Configuration Management for Software Configuration Auditing. The purpose of the software PCA is to ensure that the design and reference documentation is consistent with the as-built software product. PCA checks and matches the really implemented layout with the documented layout. Answer: C is incorrect. Functional Configuration Audit or FCA is one of the practices used in Software Configuration Management for Software Configuration Auditing. FCA occurs either at delivery or at the moment of effecting the change. A Functional Configuration Audit ensures that functional and performance attributes of a configuration item are achieved. Answer: B is incorrect. Configuration control is a procedure of the Configuration management. Configuration control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them. It supports the change of the functional and physical attributes of software at various points in time, and performs systematic control of changes to the identified attributes. Answer: A is incorrect. Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined. Baselining an attribute forces formal configuration change control processes to be effected in the event that these attributes are changed.

QUESTION 14

Which of the following plans is a comprehensive statement of consistent actions to be taken before, during, and after a disruptive event that causes a significant loss of information systems resources?

- A. Contingency plan
- B. Continuity of Operations plan

C. Disaster recovery plan

D. Business Continuity plan

Correct Answer: C

A disaster recovery plan is a complete statement of reliable actions to be taken before, during, and after a disruptive event that causes a considerable loss of information systems resources. The chief objective of a disaster recovery plan is to provide an organized way to make decisions if a disruptive event occurs. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication, and reputation protection, and should refer to the disaster recovery plan (DRP) for IT-related infrastructure recovery/continuity. Answer: D is incorrect. 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: B is incorrect. The Continuity Of Operation Plan (COOP) refers to the preparations and institutions maintained by the United States government, providing survival of federal government operations in the case of catastrophic events. It provides procedures and capabilities to sustain an organization's essential. COOP is the procedure documented to ensure persistent critical operations throughout any period where normal operations are unattainable. 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.

QUESTION 15

An asset with a value of \$600,000 is subject to a successful malicious attack threat twice a year. The asset has an exposure of 30 percent to the threat. What will be the annualized loss expectancy?

A. \$360,000

B. \$180,000

C. \$280,000

D. \$540,000

Correct Answer: A

The annualized loss expectancy will be \$360,000. Annualized loss expectancy (ALE) is the annually expected financial loss to an organization from a threat. The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE).

It is mathematically expressed as follows:

ALE = Single Loss Expectancy (SLE) * Annualized Rate of Occurrence (ARO) Here, it is as follows:

SLE = Asset value * EF (Exposure factor)

= 600,000 * (30/100)

$$= 600,000 * 0.30$$

$$= 180,000$$

$$\text{ALE} = \text{SLE} * \text{ARO}$$

$$= 180,000 * 2$$

$$= 360,000$$

Answer: C, B, and D are incorrect. These are not valid answers.

[Latest CSSLP Dumps](#)

[CSSLP PDF Dumps](#)

[CSSLP Study Guide](#)