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.pass4itsure.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

Which of the following processes does the decomposition and definition sequence of the Vee model include? Each correct answer represents a part of the solution. Choose all that apply.

A. Component integration and test

B. System security analysis

C. Security requirements allocation

D. High level software design

Correct Answer: BCD

Decomposition and definition sequence includes the following processes: System security analysis Security requirements allocation Software security requirements analysis High level software design Detailed software design Answer: A is incorrect. This process is included in the integration and verification sequence of the Vee model.

QUESTION 2

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 3

Which of the following describes a residual risk as the risk remaining after a risk mitigation has occurred?

A. DIACAP

B. SSAA

C. DAA

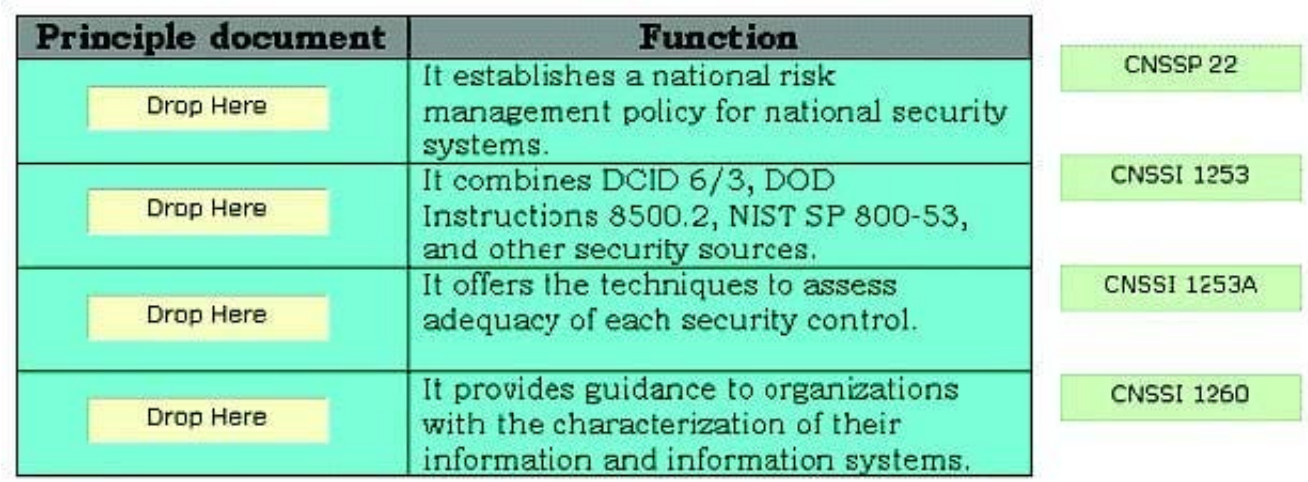
D. ISSO

Correct Answer: A

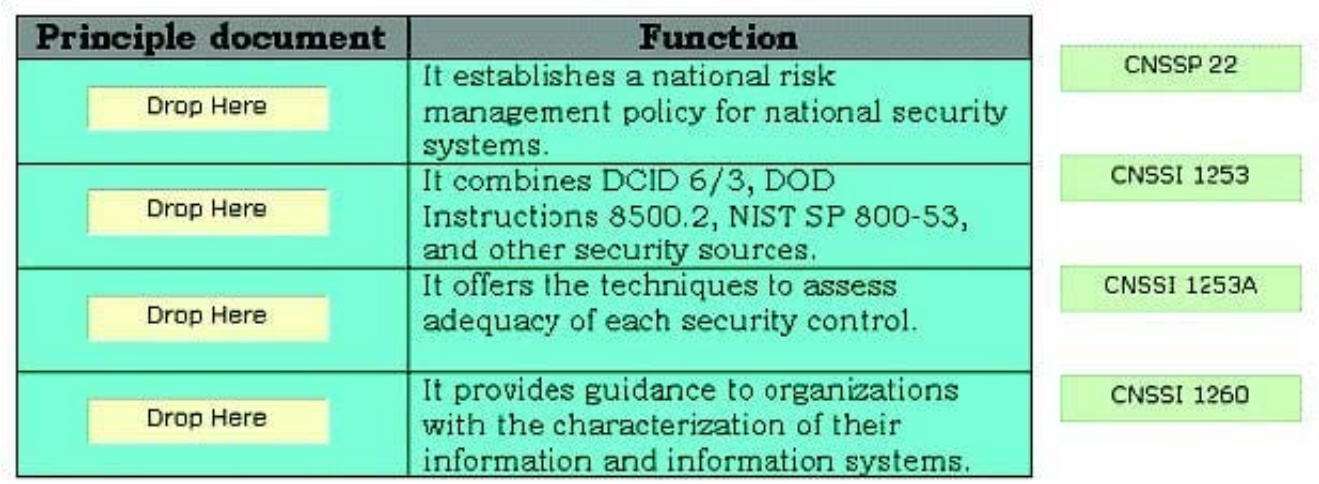
DIACAP describes a residual risk as the risk remaining after a risk mitigation has occurred. The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk. DIACAP replaced the former process, known as DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process), in 2006. DoD Instruction (DoDI) 8510.01 establishes a standard DoD-wide process with a set of activities, general tasks, and a management structure to certify and accredit an Automated Information System (AIS) that will maintain the Information Assurance (IA) posture of the Defense Information Infrastructure (DII) throughout the system\\'s life cycle.DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. It identifies four phases: 1.System Definition 2.Verification 3.Validation 4.Re-Accreditation Answer: D is incorrect. An Information System Security Officer (ISSO) plays the role of a supporter. The responsibilities of an Information System Security Officer (ISSO) are as follows: Manages the security of the information system that is slated for Certification and Accreditation (CandA). Insures the information systems configuration with the agency\\'s information security policy. Supports the information system owner/information owner for the completion of security-related responsibilities. Takes part in the formal configuration management process. Prepares Certification and Accreditation (CandA) packages. Answer: C is incorrect. The Designated Approving Authority (DAA), in the United States Department of Defense, is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. The DAA is responsible for implementing system security. The DAA can grant the accreditation and can determine that the system\\'s risks are not at an acceptable level and the system is not ready to be operational. Answer: B is incorrect. System Security Authorization Agreement (SSAA) is an information security document used in the United States Department of Defense (DoD) to describe and accredit networks and systems. The SSAA is part of the Department of Defense Information Technology Security Certification and Accreditation Process, or DITSCAP (superseded by DIACAP). The DoD instruction (issues in December 1997, that describes DITSCAP and provides an outline for the SSAA document is DODI 5200.40. The DITSCAP application manual (DoD 8510.1-M), published in July 2000, provides additional details.

QUESTION 4

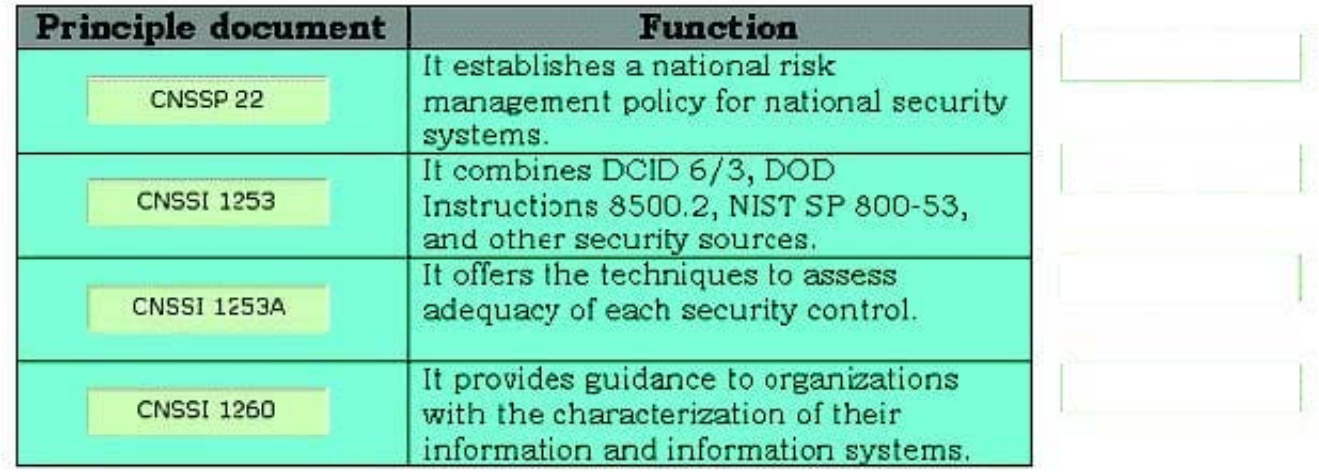
Drag and drop the appropriate principle documents in front of their respective functions.



Select and Place:



Correct Answer:



The various principle documents of transformation are as follows: CNSSP 22: It establishes a national risk management policy for national security systems. CNSSI 1199: It creates the technique in which the national security community classifies the information and information systems with regard to confidentiality, integrity, and availability. CNSSI 1253: It combines DCID 6/3, DOD Instructions 8500.2, NIST SP 800-53, and other security sources into a single cohesive repository of security controls. CNSSI 1253 A. It offers the techniques to assess adequacy of each security control. CNSSI 1260: It provides guidance to organizations with the characterization of their information and information systems. NIST 800-37, Revision 1: It defines the certification and accreditation (C and A) process. The NIST 800-37, Revision 1 is a combination of DNI, DoD, and NIST.

QUESTION 5

DoD 8500.2 establishes IA controls for information systems according to the Mission Assurance Categories (MAC) and confidentiality levels. Which of the following MAC levels requires high integrity and medium availability?

A. MAC III

B. MAC IV

C. MAC I

D. MAC II

Correct Answer: D

The various MAC levels are as follows: MAC I: It states that the systems have high availability and high integrity. MAC II: It states that the systems have high integrity and medium availability. MAC III: It states that the systems have basic integrity and availability.

QUESTION 6

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. What are the process activities of this phase? Each correct answer represents a complete solution. Choose all that apply.

A. Certification and accreditation decision

B. Continue to review and refine the SSAA

C. Perform certification evaluation of the integrated system

D. System development

E. Develop recommendation to the DAA

Correct Answer: ABCE

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. The process activities of this phase are as follows: Continue to review and refine the SSAA Perform certification evaluation of the integrated system Develop recommendation to the DAA Certification and accreditation decision Answer: D is incorrect. System development is a Phase 2 activity.

QUESTION 7

Which of the following steps of the LeGrand Vulnerability-Oriented Risk Management method determines the necessary compliance offered by risk management practices and assessment of risk levels?

A. Assessment, monitoring, and assurance

B. Vulnerability management

C. Risk assessment

D. Adherence to security standards and policies for development and deployment

Correct Answer: A

Assessment, monitoring, and assurance determines the necessary compliance that are offered by risk management practices and assessment of risk levels.

QUESTION 8

Which of the following techniques is used when a system performs the penetration testing with the objective of accessing unauthorized information residing inside a computer?

A. Biometrician

B. Van Eck Phreaking

C. Port scanning

D. Phreaking

Correct Answer: C

Port scanning identifies open doors to a computer. Hackers and crackers use this technique to obtain unauthorized information. Port scanning is the first basic step to get the details of open ports on the target system. Port scanning is used to find a hackable server with a hole or vulnerability. A port is a medium of communication between two computers. Every service on a host is identified by a unique 16-bit number called a port. A port scanner is a piece of software designed to search a network host for open ports. This is often used by administrators to check the security of their networks and by hackers to identify running services on a host with the view to compromising it. Port scanning is used to find the open ports, so that it is possible to search exploits related to that service and application. Answer: D is incorrect. Phreaking is a process used to crack the phone system. The main aim of phreaking is to avoid paying for long- distance calls. As telephone networks have become computerized, phreaking has become closely linked with computer hacking. This is sometimes called the H/P culture (with H standing for Hacking and P standing for Phreaking). Answer: A is incorrect. It is defined as a system using a physical attribute for authenticating. Only authorized users are provided access to network or application. Answer: B is incorrect. It is described as a form of eavesdropping in which special equipments are used to pick up the telecommunication signals or data within a computer device.

QUESTION 9

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

ALE = SLE * ARO

= 180,000 * 2

= 360,000

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

QUESTION 10

Fred is the project manager of the CPS project. He is working with his project team to prioritize the identified risks within the CPS project. He and the team are prioritizing risks for further analysis or action by assessing and combining the risks probability of occurrence and impact. What process is Fred completing?

A. Risk identification

B. Risk Breakdown Structure creation

C. Perform qualitative analysis

D. Perform quantitative analysis

Correct Answer: C

Qualitative ranks the probability and impact and then helps the project manager and team to determine which risks need further analysis. Perform Qualitative Risk Analysis is the process of prioritizing risks for further analysis and action. It combines risks and their probability of occurrences and ranks them accordingly. It enables organizations to improve the project\\'s performance by focusing on high-priority risks. Perform Qualitative Risk Analysis is usually a rapid and cost-effective means of establishing priorities for Plan Risk Responses. It also lays the foundation for Perform Quantitative Risk Analysis. Answer: A is incorrect. Risk identification precedes this activity. Answer: B is incorrect. This process does not describe the decomposition and organization of risks that you will complete in a risk breakdown structure. Answer: D is incorrect. Quantitative analysis is the final step of risk analysis. Note the question tells you that Fred and the team will identify risks for additional analysis.

QUESTION 11

Which of the following is the process of finding weaknesses in cryptographic algorithms and obtaining the plaintext or key from the ciphertext?

A. Cryptographer

B. Cryptography

C. Kerberos

D. Cryptanalysis

Correct Answer: D

Cryptanalysis is the process of analyzing cipher text and finding weaknesses in cryptographic algorithms. These weaknesses can be used to decipher the cipher text without knowing the secret key. Answer: C is incorrect. Kerberos is an industry standard authentication protocol used to verify user or host identity. Kerberos v5 authentication protocol is the default authentication service for Windows 2000. It is integrated into the administrative and security model, and provides secure communication between Windows 2000 Server domains and clients. Answer: A is incorrect. A cryptographer is a person who is involved in cryptography.

Answer: B is incorrect. Cryptography is a branch of computer science and mathematics. It is used for protecting information by encoding it into an unreadable format known as cipher text.

QUESTION 12

You are the project manager of the NNN project for your company. You and the project team are working together to plan the risk responses for the project. You feel that the team has successfully completed the risk response planning and now you must initiate what risk process it is. Which of the following risk processes is repeated after the plan risk responses to determine if the overall project risk has been satisfactorily decreased?

A. Quantitative risk analysis

B. Risk identification

C. Risk response implementation

D. Qualitative risk analysis

Correct Answer: A

The quantitative risk analysis process is repeated after the plan risk responses to determine if the overall project risk has been satisfactorily decreased. Answer: D is incorrect. Qualitative risk analysis is not repeated after the plan risk response process. Answer: B is incorrect. Risk identification is an ongoing process that happens throughout the project. Answer: C is incorrect. Risk response implementation is not a project management process.

QUESTION 13

You work as a project manager for BlueWell Inc. You are preparing to plan risk responses for your project with your team. How many risk response types are available for a negative risk event in the project?

A. Three

B. Seven

C. One

D. Four

Correct Answer: D

There are four risk responses available for a negative risk event. The risk response strategies for negative risks are: Avoid: It involves altering the project management plan to remove the threats completely. Transfer: It requires shifting some or all of the negative effects of a threat including the ownership of response, to a third party. Mitigate: It implies a drop in the probability and impact of an unfavorable risk event to be within suitable threshold limits. Accept: It delineates that the project plan will not be changed to deal with the risk. Management may develop a contingency plan if the risk occurs. It is used for both negative and positive risks. Answer: C is incorrect. There are four responses for negative risk

events. Answer: A is incorrect. There are four, not three, responses for negative risk events. Do not forget that acceptance can be used for negative risk events. Answer: B is incorrect. There are seven total risk responses, four of which can be used for negative risk events.

QUESTION 14

Which of the following are the initial steps required to perform a risk analysis process? Each correct answer represents a part of the solution. Choose three.

A. Valuations of the critical assets in hard costs.

B. Evaluate potential threats to the assets.

C. Estimate the potential losses to assets by determining their value.

D. Establish the threats likelihood and regularity.

Correct Answer: BCD

The main steps of performing risk analysis are as follows: Estimate the potential losses to the assets by determining their value. Evaluate the potential threats to the assets. Establish the threats probability and regularity. Answer: A is incorrect. Valuations of the critical assets in hard costs is one of the final steps taken after performing the risk analysis.

QUESTION 15

You work as the senior project manager in SoftTech Inc. You are working on a software project using configuration management. Through configuration management you are decomposing the verification system into identifiable, understandable, manageable, traceable units that are known as Configuration Items (CIs). According to you, which of the following processes is known as the decomposition process of a verification system into Configuration Items?

A. Configuration status accounting

B. Configuration identification

C. Configuration auditing

D. Configuration control

Correct Answer: B

Configuration identification is known as the decomposition process of a verification system into Configuration Items. 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. Answer: D 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. Configuration control is a means of ensuring that system changes are approved before being implemented. Only the proposed and approved changes are implemented, and the implementation is complete and accurate. Answer: A is incorrect. The configuration status accounting procedure is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time. It supports the functional and physical attributes of software at various points in time, and performs systematic control of accounting to the identified attributes for the

purpose of maintaining software integrity and traceability throughout the software development life cycle. Answer: C is incorrect. Configuration auditing is the quality assurance element of configuration management. It is occupied in the process of periodic checks to establish the consistency and completeness of accounting information and to validate that all configuration management policies are being followed. Configuration audits are broken into functional and physical configuration audits. They occur 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, while a physical configuration audit ensures that a configuration item is installed in accordance with the requirements of its detailed design documentation.