ISC

Exam CSSLP

Certified Secure Software Lifecycle Professional

Verson: Demo

[Total Questions: 10]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	4
Topic 2: Volume B	3
Topic 3: Volume C	3

Topic 1, Volume A

Question No : 1 - (Topic 1)

The Phase 4 of DITSCAP C&A is known as Post Accreditation. This phase starts after the system has been accredited in Phase 3. What are the process activities of this phase? Each correct answer represents a complete solution. Choose all that apply.

A. Security operations
B. Maintenance of the SSAA
C. Compliance validation
D. Change management
E. System operations
F. Continue to review and refine the SSAA

Answer: A,B,C,D,E

Explanation: The Phase 4 of DITSCAP C&A is known as Post Accreditation. This phase starts after the system has been accredited in the Phase 3. The goal of this phase is to continue to operate and manage the system and to ensure that it will maintain an acceptable level of residual risk. The process activities of this phase are as follows: System operations Security operations Maintenance of the SSAA Change management Compliance validation Answer: F is incorrect. It is a Phase 3 activity.

Question No : 2 - (Topic 1)

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

Answer: A

Explanation: 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 No : 3 - (Topic 1)

You work as a Security Manager for Tech Perfect Inc. In the organization, Syslog is used for computer system management and security auditing, as well as for generalized informational, analysis, and debugging messages. You want to prevent a denial of service (DoS) for the Syslog server and the loss of Syslog messages from other sources. What will you do to accomplish the task?

A. Use a different message format other than Syslog in order to accept data.
B. Enable the storage of log entries in both traditional Syslog files and a database.
C. Limit the number of Syslog messages or TCP connections from a specific source for a certain time period.
D. Encrypt rotated log files automatically using third-party or OS mechanisms.

Answer: C

Explanation: In order to accomplish the task, you should limit the number of Syslog messages or TCP connections from a specific source for a certain time period. This will prevent a denial of service (DoS) for the Syslog server and the loss of Syslog messages from other sources. Answer: D is incorrect. You can encrypt rotated log files automatically using third-party or OS mechanisms to protect data confidentiality. Answer: A is incorrect. You can use a different message format other than Syslog in order to accept data for aggregating data from hosts that do not support Syslog. Answer: B is incorrect. You can enable the storage of log entries in both traditional Syslog files and a database for creating a database storage for logs.

Question No : 4 - (Topic 1)

You work as a security engineer for BlueWell Inc. Which of the following documents will you use as a guide for the security certification and accreditation of Federal Information Systems?

A. NIST Special Publication 800-60
B. NIST Special Publication 800-53
C. NIST Special Publication 800-37
D. NIST Special Publication 800-59

Answer: C

Explanation: NIST has developed a suite of documents for conducting Certification & Accreditation (C&A). These documents are as follows: NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems.
NIST Special Publication 800-53: This document provides a guideline for security controls for Federal Information Systems. NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System. NIST Special Publication 800-59: This document is a guideline for identifying an information system as a National Security System. NIST Special Publication 800-60: This document is a guide for mapping types of information and information systems to security objectives and risk levels.

Topic 2, Volume B

Question No : 5 - (Topic 2)

You are the project manager for your organization. You are preparing for the quantitative risk analysis. Mark, a project team member, wants to know why you need to do quantitative risk analysis when you just completed qualitative risk analysis. Which one of the following statements best defines what quantitative risk analysis is?

A. Quantitative risk analysis is the process of prioritizing risks for further analysis or action by assessing and combining their probability of occurrence and impact.

B. Quantitative risk analysis is the review of the risk events with the high probability and the highest impact on the project objectives.
C. Quantitative risk analysis is the planning and quantification of risk responses based on probability and impact of each risk event.
D. Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives.

Answer: D

Explanation: Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives. It is performed on risk that have been prioritized through the qualitative risk analysis process. Answer: A is incorrect. This is actually the definition of qualitative risk analysis. Answer: B is incorrect. While somewhat true, this statement does not completely define the quantitative risk analysis process. Answer: C is incorrect. This is not a valid statement about the quantitative risk analysis process. Risk response planning is a separate project management process.

Question No : 6 DRAG DROP - (Topic 2)

Drag and drop the correct DoD Policy Series at their appropriate places.

Policy Subject Area	DoD Policy Series
General	Drop Here
IA Certification and Accreditation	Drop Here
Security Management	Drop Here
Computer Network Defense	Drop Here
IA Education, Training, and Awareness	Drop Here
Interconnectivity	Drop Here

8540
8570
8530
8520
8510
8500

Answer:

Policy Subject Area	DoD Policy Series
General	8500
IA Certification and Accreditation	8510
Security Management	8520
Computer Network Defense	8530
IA Education, Training, and Awareness	8570
Interconnectivity	8540

8540 8570 8530 8520 8510 8500

Explanation:

Policy Subject Area	DoD Policy Series
General	8500
IA Certification and Accreditation	8510
Security Management	8520
Computer Network Defense	8530
IA Education, Training, and Awareness	8570
Interconnectivity	8540

8540 8570 8530 8520 8510 8500

The various DoD policy series are as follows:

DoD Policy Series	Policy Subject Area
8500	General
8510	IA Certification and Accreditation
8520	Security Management
8530	Computer Network Defense
8540	Interconnectivity
8550	Network and Web
8560	IA Monitoring
8570	IA Education, Training, and Awareness
8580	Other (Integration)

Question No : 7 - (Topic 2)

The Project Risk Management knowledge area focuses on which of the following processes? Each correct answer represents a complete solution. Choose all that apply.

A. Risk Monitoring and Control
B. Risk Management Planning
C. Quantitative Risk Analysis
D. Potential Risk Monitoring

Answer: A,B,C

Explanation: The Project Risk Management knowledge area focuses on the following processes: Risk Management Planning Risk Identification Qualitative Risk Analysis Quantitative Risk Analysis Risk Response Planning Risk Monitoring and Control Answer: D is incorrect. There is no such process in the Project Risk Management knowledge area.

Topic 3, Volume C

Question No : 8 - (Topic 3)

Security Test and Evaluation (ST&E) is a component of risk assessment. It is useful in discovering system vulnerabilities. For what purposes is ST&E used? Each correct answer represents a complete solution. Choose all that apply.

A. To implement the design of system architecture
B. To determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy
C. To assess the degree of consistency between the system documentation and its implementation
D. To uncover design, implementation, and operational flaws that may allow the violation of security policy

Answer: B,C,D

Explanation: Security Test and Evaluation (ST&E) is a component of risk assessment. It is useful in discovering system vulnerabilities. According to NIST SP 800-42 (Guideline on

Network Security Testing), ST&E is used for the following purposes: To assess the degree of consistency between the system documentation and its implementation To determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy To uncover design, implementation, and operational flaws that may allow the violation of security policy Answer: A is incorrect. ST&E is not used for the implementation of the system architecture.

Question No : 9 - (Topic 3)

You work as a CSO (Chief Security Officer) for Tech Perfect Inc. You want to perform the following tasks: Develop a risk-driven enterprise information security architecture. Deliver security infrastructure solutions that support critical business initiatives. Which of the following methods will you use to accomplish these tasks?

A. Service-oriented modeling and architecture
B. Service-oriented modeling framework
C. Sherwood Applied Business Security Architecture
D. Service-oriented architecture

Answer: C

Explanation: SABSA (Sherwood Applied Business Security Architecture) is a framework and methodology for Enterprise Security Architecture and Service Management. SABSA is a model and a methodology for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives. The primary characteristic of the SABSA model is that everything must be derived from an analysis of the business requirements for security, especially those in which security has an enabling function through which new business opportunities can be developed and exploited. Answer: B is incorrect. The service-oriented modeling framework (SOMF) is a service-oriented development life cycle methodology. It offers a number of modeling practices and disciplines that contribute to a successful service-oriented life cycle management and modeling. The service-oriented modeling framework illustrates the major elements that identify the "what to do" aspects of a service development scheme. Answer: A is incorrect. The service-oriented modeling and architecture (SOMA) includes an analysis and design method that extends traditional object-oriented and component-based analysis and design methods to include concerns relevant to and supporting SOA. Answer: D is incorrect. The service-oriented architecture (SOA) is a flexible set of design principles used during the phases of systems development and integration.

Question No : 10 - (Topic 3)

In which of the following SDLC phases is the system's security features configured and enabled, the system is tested and installed or fielded, and the system is authorized for processing?

A. Development/Acquisition Phase
B. Operation/Maintenance Phase
C. Implementation Phase
D. Initiation Phase

Answer: C

Explanation: It is the implementation phase, in which the system's security features are configured and enabled, the system is tested and installed or fielded, and the system is authorized for processing. A design review and systems test should be performed prior to placing the system into operation to ensure that it meets security specifications. Answer: B is incorrect. In Operation/Maintenance Phase, the system performs its work. The system is almost always being continuously modified by the addition of hardware and software and by numerous other events. Answer: D is incorrect. In the initiation phase, the need for a system is expressed and the purpose of the system is documented. Answer: A is incorrect. In Development/Acquisition Phase, the system is designed, purchased, programmed, developed, or otherwise constructed.