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 64

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 65

You work as a project manager for a company. The company has started a new security software project. The software configuration management will be used throughout the lifecycle of the project. You are tasked to modify the functional features and the basic logic of the software and then make them compatible to the initial design of the project. Which of the following procedures of the configuration management will you follow to accomplish the task?

A. Configuration status accounting
B. Configuration control
C. Configuration audits
D. Configuration identification

Answer: B

Explanation:

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: C is incorrect. Configuration audits confirm that the configuration identification for a configured item is accurate, complete, and will meet specified program needs. 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. Answer: D 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. 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.

QUESTION 66

Which of the following areas of information system, as separated by Information Assurance Framework, is a collection of local computing devices, regardless of physical location, that are interconnected via local area networks (LANs) and governed by a single security policy?

A. Local Computing Environments
B. Networks and Infrastructures
C. Supporting Infrastructures
D. Enclave Boundaries

Answer: D
Explanation:
The areas of information system, as separated by Information Assurance Framework, are as follows: Local Computing Environments: This area includes servers, client workstations, operating system, and applications. Enclave Boundaries: This area consists of collection of local computing devices, regardless of physical location, that are interconnected via local area networks (LANs) and governed by a single security policy. Networks and Infrastructures: This area provides the network connectivity between enclaves. It includes operational area networks (OANs), metropolitan area networks (MANs), and campus area networks (CANs). Supporting Infrastructures: This area provides security services for networks, client workstations, Web servers, operating systems, applications, files, and single-use infrastructure machines

QUESTION 67

Which of the following is a signature-based intrusion detection system (IDS) ?

A. RealSecure
B. StealthWatch
C. Tripwire
D. Snort

Answer: D
Explanation:

Snort is a signature-based intrusion detection system. Snort is an open source network intrusion prevention and detection system that operates as a network sniffer. It logs activities of the network that is matched with the predefined signatures. Signatures can be designed for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP). The three main modes in which Snort can be configured are as follows: Sniffer mode: It reads the packets of the network and displays them in a continuous stream on the console. Packet logger mode: It logs the packets to the disk. Network intrusion detection mode: It is the most complex and configurable configuration, allowing Snort to analyze network traffic for matches against a user-defined rule set. Answer: B is incorrect. StealthWatch is a behavior-based intrusion detection system. Answer: A is incorrect. RealSecure is a network-based IDS that monitors TCP, UDP and ICMP traffic and is configured to look for attack patterns. Answer: C is incorrect. Tripwire is a file integrity checker for UNIX/Linux that can be used for host-based intrusion detection.

QUESTION 68

Which of the following statements about the availability concept of Information security management is true?

A. It ensures that modifications are not made to data by unauthorized personnel or processes.
B. It determines actions and behaviors of a single individual within a system.
C. It ensures reliable and timely access to resources.
D. It ensures that unauthorized modifications are not made to data by authorized personnel or processes.

Answer: C
Explanation:
The concept of availability ensures reliable and timely access to data or resources. In other words, availability ensures that the systems are up and running when needed. The availability concept also ensures that the security services are in working order. Answer: A and D are incorrect. The concept of integrity ensures that modifications are not made to data by unauthorized personnel or processes. It also ensures that unauthorized modifications are not made to data by authorized personnel or processes. Answer: B is incorrect. Accountability determines the actions and behaviors of an individual within a system, and identifies that particular individual. Audit trails and logs support accountability.

QUESTION 69

A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. Which of the following are required to be addressed in a well designed policy? Each correct answer represents a part of the solution. Choose all that apply.

A. What is being secured?
B. Where is the vulnerability, threat, or risk?
C. Who is expected to exploit the vulnerability?
D. Who is expected to comply with the policy?

Answer: ABD
Explanation:
A security policy is an overall general statement produced by senior management (or a selected

policy board or committee) that dictates what role security plays within the organization. A well designed policy addresses the following: What is being secured? - Typically an asset. Who is expected to comply with the policy? - Typically employees. Where is the vulnerability, threat, or risk? - Typically an issue of integrity or responsibility.

QUESTION 70

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: ABCDE
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 71

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.

QUESTION 72

Which of the following is an example of over-the-air (OTA) provisioning in digital rights management?

A. Use of shared secrets to initiate or rebuild trust.
B. Use of software to meet the deployment goals.
C. Use of concealment to avoid tampering attacks.
D. Use of device properties for unique identification.

Answer: A
Explanation:
Over- the- air provisioning is a mechanism to deploy MIDlet suites over a network. It is a method of distributing MIDlet suites. MIDlet suite providers install their MIDlet suites on Web servers and provide a hypertext link for downloading. A user can use this link to download the MIDlet suite either through the Internet microbrowser or through WAP on his device. Over-the-air provisioning is required for end-to-end encryption or other security purposes in order to deliver copyrighted software to a mobile device. For example, use of shared secrets to initiate or rebuild trust. Answer D and C are incorrect. The use of device properties for unique identification and the use of concealment to avoid tampering attacks are the security challenges in digital rights management (DRM). Answer B is incorrect. The use of software and hardware to meet the deployment goals is a distracter.

QUESTION 73
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

Answer: ABCE
Explanation:
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 74
Which of the following DoD directives is referred to as the Defense Automation Resources Management Manual?

A. DoD 8910.1
B. DoD 7950.1-M
C. DoDD 8000.1
D. DoD 5200.22-M
E. DoD 5200.1-R

Answer: B
Explanation:
The various DoD directives are as follows:

DoD 5200.1-R: This DoD directive refers to the 'Information Security Program Regulation'. DoD 5200.22-M: This DoD directive refers the 'National Industrial Security Program Operating Manual'.