ISC.CSSLP.v2023-02-09.q213

Exam Code:	CSSLP
Exam Name:	Certified Secure Software Lifecycle Professional Practice Test
Certification Provider:	ISC
Free Question Number:	213
Version:	v2023-02-09
# of views:	2537
# of Questions views:	2130
https://www.freeqas.com/qa/ISC/CSSLP/ISC.CSSLP.v2023-02-09.q213.html	

NEW QUESTION: 1
Which of the following is the most secure method of authentication?
A. Biometrics
B. Username and password
C. Anonymous
D. Smart card
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation: Biometrics is a method of authentication that uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user. Nowadays, the usage of biometric devices such as hand scanners and retinal scanners is becoming more common in the business environment. It is the most secure method of authentication. AnswerB is incorrect.
Username and password is the least secure method of authentication in comparison of smart card and biometrics authentication. Username and password can be intercepted. AnswerD is incorrect. Smart card authentication is not as reliable as biometrics authentication. Answer: C is incorrect. Anonymous authentication does not provide security as a user can log on to the system anonymously and he is not prompted for credentials.

NEW QUESTION: 2
An attacker exploits actual code of an application and uses a security hole to carry out an attack before the application vendor knows about the vulnerability. Which of the following types of attack is this?
A. Replay
B. Zero-day
C. Man-in-the-middle
D. Denial-of-Service

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation: A zero-day attack, also known as zero-hour attack, is a computer threat that tries to exploit computer application vulnerabilities which are unknown to others, undisclosed to the software vendor, or for which no security fix is available. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software vendor knows about the vulnerability. User awareness training is the most effective technique to mitigate such attacks. AnswerA is incorrect. A replay attack is a type of attack in which attackers capture packets containing passwords or digital signatures whenever packets pass between two hosts on a network. In an attempt to obtain an authenticated connection, the attackers then resend the captured packet to the system. In this type of attack, the attacker does not know the actual password, but can simply replay the captured packet. Answer: C is incorrect.

Man-in-the-middle attacks occur when an attacker successfully inserts an intermediary software or program between two communicating hosts. The intermediary software or program allows attackers to listen to and modify the communication packets passing between the two hosts. The software intercepts the communication packets and then sends the information to the receiving host. The receiving host responds to the software, presuming it to be the legitimate client.

AnswerD is incorrect. A Denial-of- Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as network saturation attack or bandwidth consumption attack.

Attackers perform DoS attacks by sending a large number of protocol packets to a network.

NEW QUESTION: 3

Which of the following is an example of penetration testing?

A. Implementing NIDS on a network

B. Implementing HIDS on a computer

C. Simulating an actual attack on a network

D. Configuring firewall to block unauthorized traffic

Answer: C (LEAVE A REPLY)

Penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source, known as a Black Hat Hacker, or Cracker. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The intent of a penetration testing is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered. It is a component of a full security audit. Answer A, B, and D are incorrect. Implementing NIDS and HIDS and configuring firewall to block unauthorized traffic are not examples of penetration testing.

NEW QUESTION: 4
Which of the following specifies access privileges to a collection of resources by using the URL mapping?
A. Code Access Security
B. Security constraint
C. Configuration Management
D. Access Management
E. Explanation:
Security constraint is a type of declarative security, which specifies the protection of web content. It also specifies access privileges to a collection of resources by using the URL mapping. A deployment descriptor is used to define the security constraint. Security constraint includes the following elements: Web resource collection Authorization constraint User data constraint
Answer: B (LEAVE A REPLY)
is incorrect. Code Access Security (CAS), in the Microsoft .NET framework, is Microsoft's solution to prevent untrusted code from performing privileged actions. When the CLR (common language runtime) loads an assembly it will obtain evidence for the assembly and use this to identify the code group that the assembly belongs to. A code group contains a permission set (one or more permissions). Code that performs a privileged action will perform a code access demand, which will cause the CLR to walk up the call stack and examine the permission set granted to the assembly of each method in the call stack. The code groups and permission sets are determined by the administrator of the machine who defines the security policy. Answer D is incorrect. Access Management is used to grant authorized users the right to use a service, while preventing access to non- authorized users. The Access Management process essentially executes policies defined in IT Security Management. It is sometimes also referred to as Rights Management or Identity Management. It is part of Service Operation and the owner of Access Management is the Access Manager. Access Management is added as a new process to ITIL V3. The sub-processes of Access Management are as follows: Maintain Catalogue of User Roles and Access Profiles Manage User Access Requests Answer C is incorrect. Configuration Management (CM) is an Information Technology Infrastructure Library (ITIL) IT Service Management (ITSM) process. It tracks all of the individual Configuration Items (CI) in an IT system, which may be as simple as a single server, or as complex as the entire IT department. In large organizations a configuration manager may be appointed to oversee and manage the CM process.

NEW QUESTION: 5
Which of the following organizations assists the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies?
A. OMB
B. NIST
C. NSA/CSS
D. DCAA

Answer: A (LEAVE A REPLY)

The Office of Management and Budget (OMB) is a Cabinet-level office, and is the largest office within the Executive Office of the President (EOP) of the United States. The current OMB Director is Peter Orszag and was appointed by President Barack Obama. The OMB's predominant mission is to assist the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies. In helping to formulate the President's spending plans, the OMB evaluates the effectiveness of agency programs, policies, and procedures, assesses competing funding demands among agencies, and sets funding priorities. The OMB ensures that agency reports, rules, testimony, and proposed legislation are consistent with the President's Budget and with Administration policies. Answer D is incorrect. The DCAA has the aim to monitor contractor costs and perform contractor audits. Answer C is incorrect. The National Security Agency/Central Security Service (NSA/CSS) is a crypto-logic intelligence agency of the United States government. It is administered as part of the United States Department of Defense. NSA is responsible for the collection and analysis of foreign communications and foreign signals intelligence, which involves cryptanalysis. NSA is also responsible for protecting U.S. government communications and information systems from similar agencies elsewhere, which involves cryptography. NSA is a key component of the U.S. Intelligence Community, which is headed by the Director of National Intelligence. The Central Security Service is a co-located agency created to coordinate intelligence activities and cooperation between NSA and U.S. military cryptanalysis agencies. NSA's work is limited to communications intelligence. It does not perform field or human intelligence activities. Answer B is incorrect. The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.

NEW QUESTION: 6

You are responsible for network and information security at a large hospital. It is a significant concern that any change to any patient record can be easily traced back to the person who made that change. What is this called?

A. Availability

B. Confidentiality

C. Non repudiation

D. Data Protection

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation: Non repudiation refers to mechanisms that prevent a party from falsely denying involvement in some data transaction.

NEW QUESTION: 7
A number of security patterns for Web applications under the DARPA contract have been developed by Kienzle, Elder, Tyree, and Edwards-Hewitt. Which of the following patterns are applicable to aspects of authentication in Web applications?b Each correct answer represents a complete solution. Choose all that apply.
A. Authenticated session
B. Secure assertion
C. Partitioned application
D. Password authentication
E. Account lockout
F. Password propagation
Answer: A,D,E,F (LEAVE A REPLY)
Explanation/Reference:
Explanation: The various patterns applicable to aspects of authentication in the Web applications are as follows: Account lockout: It implements a limit on the incorrect password attempts to protect an account from automated password-guessing attacks. Authenticated session: It allows a user to access more than one access-restricted Web page without re-authenticating every page. It also integrates user authentication into the basic session model. Password authentication: It provides protection against weak passwords, automated password-guessing attacks, and mishandling of passwords. Password propagation:
It offers a choice by requiring that a user's authentication credentials be verified by the database before providing access to that user's data. AnswerB and C are incorrect. Secure assertion and partitioned application patterns are applicable to software assurance in general.

NEW QUESTION: 8
Which of the following terms ensures that no intentional or unintentional unauthorized modification is made to data?
A. Non-repudiation
B. Integrity
C. Authentication
D. Confidentiality
Answer: B (LEAVE A REPLY)
Integrity ensures that no intentional or unintentional unauthorized modification is made to data. Answer D is incorrect. Confidentiality refers to the protection of data against unauthorized access. Administrators can provide confidentiality by encrypting data. Answer A is incorrect. Non-repudiation is a mechanism to prove that the sender really sent this message. Answer C is incorrect. Authentication is the process of verifying the identity of a person or network host.

NEW QUESTION: 9
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. In order to do so, he performs the following steps of the pre-

attack phase successfully: Information gathering Determination of network range Identification of active systems Location of open ports and applications Now, which of the following tasks should he perform next?

A. Perform OS fingerprinting on the We-are-secure network.

B. Map the network of We-are-secure Inc.

C. Install a backdoor to log in remotely on the We-are-secure server.

D. Fingerprint the services running on the we-are-secure network.

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation: John will perform OS fingerprinting on the We-are-secure network. Fingerprinting is the easiest way to detect the Operating System (OS) of a remote system. OS detection is important because, after knowing the target system's OS, it becomes easier to hack into the system. The comparison of data packets that are sent by the target system is done by fingerprinting. The analysis of data packets gives the attacker a hint as to which operating system is being used by the remote system. There are two types of fingerprinting techniques as follows: 1.Active fingerprinting 2.Passive fingerprinting In active fingerprinting ICMP messages are sent to the target system and the response message of the target system shows which OS is being used by the remote system. In passive fingerprinting the number of hops reveals the OS of the remote system. Answer: D and B are incorrect. John should perform OS fingerprinting first, after which it will be easy to identify which services are running on the network since there are many services that run only on a specific operating system. After performing OS fingerprinting, John should perform networking mapping. Answer: C is incorrect. This is a pre-attack phase, and only after gathering all relevant knowledge of a network should John install a backdoor.

NEW QUESTION: 10

Which of the following requires all general support systems and major applications to be fully certified and accredited before these systems and applications are put into production? Each correct answer represents a part of the solution. Choose all that apply.

A. NIST

B. Office of Management and Budget (OMB)

C. FIPS

D. FISMA

Answer: B,D (LEAVE A REPLY)

FISMA and Office of Management and Budget (OMB) require all general support systems and major applications to be fully certified and accredited before they are put into production. General support systems and major applications are also referred to as information systems and are required to be reaccredited every three years. Answer A is incorrect. The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and

technology in ways that enhance economic security and improve quality of life. Answer C is incorrect. The Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States federal government for use by all nonmilitary government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community (ANSI, IEEE, ISO, etc.). Some FIPS standards were originally developed by the U.S. government. For instance, standards for encoding data (e.g., country codes), but more significantly some encryption standards, such as the Data Encryption Standard (FIPS 46-3) and the Advanced Encryption Standard (FIPS 197). In 1994, NOAA (Noaa) began broadcasting coded signals called FIPS (Federal Information Processing System) codes along with their standard weather broadcasts from local stations. These codes identify the type of emergency and the specific geographic area (such as a county) affected by the emergency.

NEW QUESTION: 11
Which of the following is an attack with IP fragments that cannot be reassembled?
A. Password guessing attack
B. Teardrop attack
C. Dictionary attack
D. Smurf attack
Answer: B (LEAVE A REPLY)
Teardrop is an attack with IP fragments that cannot be reassembled. In this attack, corrupt packets are sent to the victim's computer by using IP's packet fragmentation algorithm. As a result of this attack, the victim's computer might hang. Answer D is incorrect. Smurf is an ICMP attack that involves spoofing and flooding. Answer C is incorrect. Dictionary attack is a type of password guessing attack. This type of attack uses a dictionary of common words to find out the password of a user. It can also use common words in either upper or lower case to find a password. There are many programs available on the Internet to automate and execute dictionary attacks. Answer A is incorrect. A password guessing attack occurs when an unauthorized user tries to log on repeatedly to a computer or network by guessing usernames and passwords. Many password guessing programs that attempt to break passwords are available on the Internet. Following are the types of password guessing attacks: Brute force attack Dictionary attack

NEW QUESTION: 12
Which of the following processes describes the elements such as quantity, quality, coverage, timelines, and availability, and categorizes the different functions that the system will need to perform in order to gather the documented mission/business needs?
A. Human factors
B. Functional requirements
C. Performance requirements
D. Operational scenarios
Answer: B (LEAVE A REPLY)

Explanation/Reference:
Explanation: The functional requirements categorize the different functions that the system will need to perform in order to gather the documented mission/business needs. The functional requirements describe the elements such as quantity, quality, coverage, timelines, and availability.
AnswerC is incorrect. The performance requirements comprise of speed, throughput, accuracy, humidity
tolerances, mechanical stresses such as vibrations or noises. AnswerA is incorrect. Human factor consists of factors, which affect the operation of the system or component, such as design space, eye movement, or ergonomics. AnswerD is incorrect. The operational scenarios provide assistance to the system designers and form the basis of major events in the acquisition phases, such as testing the products for system integration. The customer classifies and defines the operational scenarios, which indicate the range of anticipated uses of system products.

NEW QUESTION: 13
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
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation: 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 AnswerD 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 & Accreditation (C&A). 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 & Accreditation (C&A) packages. AnswerC 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. AnswerB 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.

NEW QUESTION: 14
The Phase 1 of DITSCAP C&A is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. What are the process activities of this phase? Each correct answer represents a complete solution. Choose all that apply.
A. Negotiation
B. Registration
C. Document mission need
D. Initial Certification Analysis
Answer: A,B,C (LEAVE A REPLY)
Explanation/Reference:
Explanation: The Phase 1 of DITSCAP C&A is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. The Phase 1 starts with the input of the mission need. This phase comprises three process activities: Document mission need Registration Negotiation
Answer D is incorrect. Initial Certification Analysis is a Phase 2 activity.

NEW QUESTION: 15
Which of the following refers to the ability to ensure that the data is not modified or tampered with?
A. Integrity
B. Availability
C. Non-repudiation
D. Confidentiality
Answer: A (LEAVE A REPLY)

Explanation/Reference:
Explanation: Integrity refers to the ability to ensure that the data is not modified or tampered with. Integrity means that data cannot be modified without authorization. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a Web site, when someone is able to cast a very large number of votes in an online poll, and so on. AnswerD is incorrect. Confidentiality is the property of preventing disclosure of information to unauthorized individuals or systems. Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. AnswerB is incorrect. Availability means that data must be available whenever it is needed. AnswerC is incorrect. Non-repudiation is the concept of ensuring that a party in a dispute cannot refuse to acknowledge, or refute the validity of a statement or contract. As a service, it provides proof of the integrity and origin of data. Although this concept can be applied to any transmission, including television and radio, by far the most common application is in the verification and trust of signatures.

NEW QUESTION: 16
Mark works as a Network Administrator for NetTech Inc. The company has a Windows 2000 domain- based network. Users report that they are unable to log on to the network. Mark finds that accounts are locked out due to multiple incorrect log on attempts. What is the most likely cause of the account lockouts?
A. Spoofing
B. Brute force attack
C. SYN attack
D. PING attack
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: Brute force attack is the most likely cause of the account lockouts. In a brute force attack, unauthorized users attempt to log on to a network or a computer by using multiple possible user names and passwords. Windows 2000 and other network operating systems have a security feature that locks a user account if the number of failed logon attempts occur within a specified period of time, based on the security policy lockout settings. AnswerA 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. AnswerC is incorrect. A SYN attack affects computers running on the TCP/IP protocol. It is a protocol-level attack that can render a computer's network services unavailable. A SYN attack is also known as SYN flooding.

Answer: D is incorrect. When a computer repeatedly sends ICMP echo requests to another computer, it is known as a PING attack.

NEW QUESTION: 17
Which of the following terms refers to the protection of data against unauthorized access?
A. Integrity
B. Recovery
C. Auditing
D. Confidentiality
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation: Confidentiality is a term that refers to the protection of data against unauthorized access.
Administrators can provide confidentiality by encrypting data. Symmetric encryption is a relatively fast encryption method. Hence, this method of encryption is best suited for encrypting large amounts of data such as files on a computer. AnswerA is incorrect. Integrity ensures that no intentional or unintentional unauthorized modification is made to data. AnswerC is incorrect. Auditing is used to track user accounts for file and object access, logon attempts, system shutdown etc. This enhances the security of the network.
Before enabling auditing, the type of event to be audited should be specified in the Audit Policy in User Manager for Domains.

NEW QUESTION: 18
Which of the following federal agencies has the objective to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life?
A. National Security Agency (NSA)
B. National Institute of Standards and Technology (NIST)
C. United States Congress
D. Committee on National Security Systems (CNSS)
Answer: (SHOW ANSWER)
The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory which is a non-

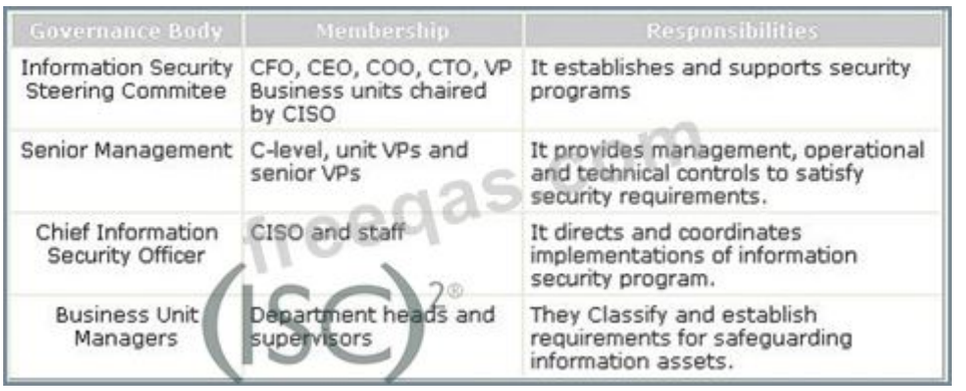
regulatory agency of the United States Department of Commerce. The institute's official mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. Answer D is incorrect. The Committee on National Security Systems (CNSS) is a United States intergovernmental organization that sets policy for the security of the US security systems. The CNSS holds discussions of policy issues, sets national policy, directions, operational procedures, and guidance for the information systems operated by the U.S. Government, its contractors, or agents that contain classified information, involve intelligence activities, involve cryptographic activities related to national security, etc. Answer A is incorrect. The National Security Agency/Central Security Service (NSA/CSS) is a crypto-logic intelligence agency of the United States government. It is administered as part of the United States Department of Defense. NSA is responsible for the collection and analysis of foreign communications and foreign signals intelligence, which involves cryptanalysis. NSA is also responsible for protecting U.S. government communications and information systems from similar agencies elsewhere, which involves cryptography. NSA is a key component of the U.S. Intelligence Community, which is headed by the Director of National Intelligence. The Central Security Service is a co-located agency created to coordinate intelligence activities and cooperation between NSA and U.S. military cryptanalysis agencies. NSA's work is limited to communications intelligence. It does not perform field or human intelligence activities. Answer C is incorrect. The United States Congress is the bicameral legislature of the federal government of the United States of America. It consists of the Senate and the House of Representatives. The Congress meets in the United States Capitol in Washington, D.C. Both senators and representatives are chosen through direct election. Each of the 435 members of the House of Representatives represents a district and serves a two-year term. House seats are apportioned among the states by population. The 100 Senators serve staggered six-year terms. Each state has two senators, regardless of population. Every two years, approximately one-third of the Senate is elected at a time. The United States Congress main function is to make laws. The Office of the Law Revision Counsel organizes and publishes the United States Code (USC). It is a consolidation and codification by subject matter of the general and permanent laws of the United States.

NEW QUESTION: 19
Which of the following phases of DITSCAP includes the activities that are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle?
A. Phase 2, Verification
B. Phase 3, Validation
C. Phase 1, Definition
D. Phase 4, Post Accreditation Phase
Answer: D (LEAVE A REPLY)
Explanation/Reference:

Explanation: Phase 4, Post Accreditation Phase, of the DITSCAP includes the activities that are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle. AnswerC is incorrect. Phase 1, Definition, focuses on understanding the mission, the environment, and the architecture in order to determine the security requirements and level of effort necessary to achieve accreditation. Answer A is incorrect. Phase 2, Verification, verifies the evolving or modified system's compliance with the information agreed on in the System Security Authorization Agreement (SSAA). Answer: B is incorrect. Phase 3 validates the compliance of a fully integrated system with the information stated in the SSAA.

NEW QUESTION: 20
Which of the following approaches can be used to build a security program? Each correct answer represents a complete solution. Choose all that apply.
A. Right-Up Approach
B. Left-Up Approach
C. Top-Down Approach
D. Bottom-Up Approach
Answer: C,D (LEAVE A REPLY)
Top-Down Approach is an approach to build a security program. The initiation, support, and direction come from the top management and work their way through middle management and then to staff members. It is treated as the best approach. This approach ensures that the senior management, who is ultimately responsible for protecting the company assets, is driving the program. Bottom-Up Approach is an approach to build a security program. The lower-end team comes up with a security control or a program without proper management support and direction. It is less effective and doomed to fail. Answer A and B are incorrect. No such types of approaches exist

NEW QUESTION: 21
Which of the following governance bodies directs and coordinates implementations of the information security program?
A. Chief Information Security Officer
B. Information Security Steering Committee
C. Business Unit Manager
D. Senior Management
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation: Chief Information Security Officer directs and coordinates implementations of the information security program. The governance roles and responsibilities are mentioned below in the table:



Governance Body	Membership	Responsibilities
Information Security Steering Commitee	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.

NEW QUESTION: 22
Which of the following security objectives are defined for information and information systems by the FISMA? Each correct answer represents a part of the solution. Choose all that apply.
A. Authenticity
B. Availability
C. Integrity
D. Confidentiality
Answer: B,C,D (LEAVE A REPLY)
Explanation/Reference:
Explanation: FISMA defines the following three security objectives for information and information systems:
Confidentiality: It means that the data should only be accessible to authorized users. Access includes printing, displaying, and other such forms of disclosure, including simply revealing the existence of an object. Integrity: It means that only authorized users are able to modify data. Modification admits changing, changing the status, deleting, and creating. Availability: It means that the data should only be available to authorized users. AnswerA is incorrect. Authenticity is not defined by the FISMA as one of the security objectives for information and information systems.

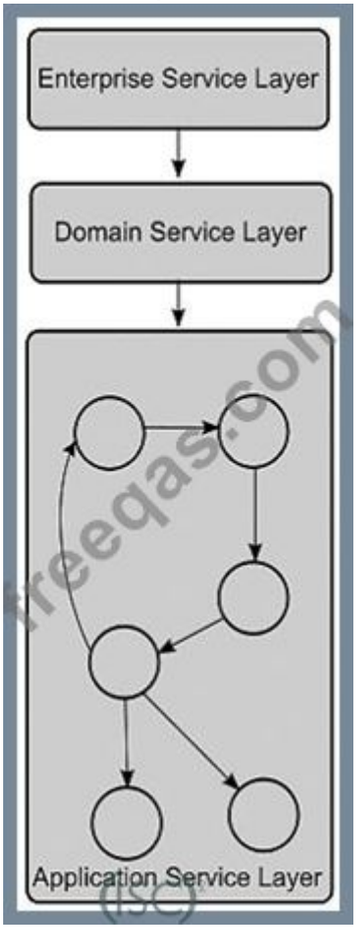
NEW QUESTION: 23
Which of the following test methods has the objective to test the IT system from the viewpoint of a threat-source and to identify potential failures in the IT system protection schemes?
A. Security Test and Evaluation (ST&E)
B. Penetration testing
C. Automated vulnerability scanning tool
D. On-site interviews
Answer: B (LEAVE A REPLY)
The goal of penetration testing is to examine the IT system from the perspective of a threat-source, and to identify potential failures in the IT system protection schemes. Penetration testing, when performed in the risk assessment process, is used to assess an IT system's capability to survive with the intended attempts to thwart system security. Answer A is incorrect. The objective of ST&E is to ensure that the applied controls meet the approved security specification for the

software and hardware and implement the organization's security policy or meet industry standards.

NEW QUESTION: 24
Which of the following NIST documents provides a guideline for identifying an information system as a National Security System?
A. NIST SP 800-37
B. NIST SP 800-59
C. NIST SP 800-53
D. NIST SP 800-60
E. NIST SP 800-53A
Answer: B (LEAVE A REPLY)
Explanation/Reference:
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.

NEW QUESTION: 25
Which of the following security architectures defines how to integrate widely disparate applications for a world that is Web-based and uses multiple implementation platforms?
A. Sherwood Applied Business Security Architecture
B. Enterprise architecture
C. Service-oriented architecture
D. Service-oriented modeling and architecture
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: In computing, a service-oriented architecture (SOA) is a flexible set of design principles used during the phases of systems development and integration. A deployed SOA-based architecture will provide a loosely-integrated suite of services that can be used within multiple business domains. SOA also generally provides a way for consumers of services, such as web-based applications, to be aware of available SOA-based services. For example, several disparate departments within a company may develop and deploy SOA services in different

implementation languages; their respective clients will benefit from a well understood, well defined interface to access them. XML is commonly used for interfacing with SOA services, though this is not required. SOA defines how to integrate widely disparate applications for a world that is Web-based and uses multiple implementation platforms. Rather than defining an API, SOA defines the interface in terms of protocols and functionality. An endpoint is the entry point for such an SOA implementation.



(Layer interaction in Service-oriented architecture) AnswerA is incorrect. 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. AnswerD 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. AnswerB is incorrect. Enterprise architecture describes the terminology, the composition of subsystems, and their relationships with the external environment, and the guiding principles for the design and evolution of an enterprise.

NEW QUESTION: 26

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

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation: 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.

NEW QUESTION: 27

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

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Explanation: 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 Commitee	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.

NEW QUESTION: 28

You work as a security manager for BlueWell Inc. You are performing the external vulnerability testing, or penetration testing to get a better snapshot of your organization's security posture.

Which of the following penetration testing techniques will you use for searching paper disposal areas for unshredded or otherwise improperly disposed-of reports?

A. Sniffing

B. Scanning and probing

C. Dumpster diving

D. Demon dialing

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation: Dumpster diving technique is used for searching paper disposal areas for unshredded or otherwise improperly disposed-of reports. Answer B is incorrect. In scanning and probing technique, various scanners, like a port scanner, can reveal information about a network's infrastructure and enable an intruder to access the network's unsecured ports. Answer: D is incorrect. Demon dialing technique automatically tests every phone line in an exchange to try to locate modems that are attached to the network. Answer: A is incorrect. In sniffing technique, protocol analyzer can be used to capture data packets that are later decoded to collect information such as passwords or infrastructure configurations.

NEW QUESTION: 29

Which of the following types of signatures is used in an Intrusion Detection System to trigger on attacks that attempt to reduce the level of a resource or system, or to cause it to crash?

A. Access

B. Benign

C. DoS

D. Reconnaissance

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation: Following are the basic categories of signatures: Informational (benign): These types of signatures trigger on normal network activity. For example: ICMP echo requests The opening or closing of TCP or UDP connections Reconnaissance: These types of signatures trigger on attacks that uncover resources and hosts that are reachable, as well as any possible vulnerabilities that they might contain. For example: Reconnaissance attacks include ping sweeps DNS queries Port scanning Access: These types of signatures trigger on access attacks, which include unauthorized access, unauthorized escalation of privileges, and access to protected or sensitive data. For example:

Back Orifice A Unicode attack against the Microsoft IIS NetBus DoS: These types of signatures trigger on attacks that attempt to reduce the level of a resource or system, or to cause it to crash. For example: TCP SYN floods The Ping of Death Smurf Fraggle Trinoo Tribe Flood Network

NEW QUESTION: 30

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
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: The Phase 3 of DITSCAP C&A 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. AnswerC is incorrect. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements.
AnswerA is incorrect. The goal of this phase is to obtain a fully integrated system for certification testing
and accreditation. AnswerB is incorrect. This phase ensures that it will maintain an acceptable level of residual risk.

NEW QUESTION: 31
Which of the following authentication methods is used to access public areas of a Web site?
A. Anonymous authentication
B. Biometrics authentication
C. Mutual authentication
D. Multi-factor authentication
Answer: A (LEAVE A REPLY)
Anonymous authentication is an authentication method used for Internet communication. It provides limited access to specific public folders and directory information or public areas of a Web site. It is supported by all clients and is used to access unsecured content in public folders. An administrator must create a user account in IIS to enable the user to connect anonymously. Answer D is incorrect. Multi-factor authentication involves a combination of multiple methods of authentication. For example, an authentication method that uses smart cards as well as usernames and passwords can be referred to as multi-factor authentication. Answer C is incorrect. Mutual authentication is a process in which a client process and server are required to prove their identities to each other before performing any application function. The client and server identities can be verified through a trusted third party and use shared secrets as in the case of Kerberos v5. The MS-CHAP v2 and EAP-TLS authentication methods support mutual authentication. Answer B is incorrect. Biometrics authentication uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user.

NEW QUESTION: 32
Which of the following are the types of access controls? Each correct answer represents a complete solution. Choose three.
A. Physical
B. Technical
C. Administrative
D. Automatic
Answer: A,B,C (LEAVE A REPLY)
Security guards, locks on the gates, and alarms come under physical access control. Policies and procedures implemented by an organization come under administrative access control. IDS systems, encryption, network segmentation, and antivirus controls come under technical access control. Answer D is incorrect. There is no such type of access control as automatic control.

NEW QUESTION: 33
You work as a system engineer for BlueWell Inc. You want to verify that the build meets its data requirements, and correctly generates each expected display and report. Which of the following tests will help you to perform the above task?
A. Performance test
B. Functional test
C. Reliability test
D. Regression test
Answer: B (LEAVE A REPLY)
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.

NEW QUESTION: 34
The mission and business process level is the Tier 2. What are the various Tier 2 activities? Each correct answer represents a complete solution. Choose all that apply.

A. Developing an organization-wide information protection strategy and incorporating high-level information security requirements
B. Defining the types of information that the organization needs, to successfully execute the stated missions and business processes
C. Specifying the degree of autonomy for the subordinate organizations
D. Defining the core missions and business processes for the organization
E. Prioritizing missions and business processes with respect to the goals and objectives of the organization
Answer: A,B,C,D,E (LEAVE A REPLY)
Explanation/Reference:
Explanation: The mission and business process level is the Tier 2. It addresses risks from the mission and business process perspective. It is guided by the risk decisions at Tier 1. The various Tier 2 activities are as follows: It defines the core missions and business processes for the organization. It also prioritizes missions and business processes, with respect to the goals and objectives of the organization. It defines the types of information that an organization requires, to successfully execute the stated missions and business processes. It helps in developing an organization-wide information protection strategy and incorporating high-level information security requirements. It specifies the degree of autonomy for the subordinate organizations.

NEW QUESTION: 35
Which of the following methods can be helpful to eliminate social engineering threat? Each correct answer represents a complete solution. Choose three.
A. Password policies
B. Data classification
C. Data encryption
D. Vulnerability assessments
Answer: A,B,D (LEAVE A REPLY)
Explanation/Reference:
Explanation: The following methods can be helpful to eliminate social engineering threat: Password policies Vulnerability assessments Data classification Password policy should specify that how the password can be shared. Company should implement periodic penetration and vulnerability assessments.
These assessments usually consist of using known hacker tools and common hacker techniques to breach a network security. Social engineering should also be used for an accurate assessment. Since social engineers use the knowledge of others to attain information, it is essential to have a data classification model in place that all employees know and follow. Data classification assigns level of sensitivity of company information. Each classification level specifies that who can view and edit data, and how it can be shared.

NEW QUESTION: 36
Which of the following roles is also known as the accreditor?

A. Data owner
B. Chief Risk Officer
C. Chief Information Officer
D. Designated Approving Authority
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation: Designated Approving Authority (DAA) is also known as the accreditor. Answer: A is incorrect.
The data owner (information owner) is usually a member of management, in charge of a specific business unit, and is ultimately responsible for the protection and use of a specific subset of information. Answer: B is incorrect. A Chief Risk Officer (CRO) is also known as Chief Risk Management Officer (CRMO). The Chief Risk Officer or Chief Risk Management Officer of a corporation is the executive accountable for enabling the efficient and effective governance of significant risks, and related opportunities, to a business and its various segments. Risks are commonly categorized as strategic, reputational, operational, financial, or compliance-related. CRO's are accountable to the Executive Committee and The Board for enabling the business to balance risk and reward. In more complex organizations, they are generally responsible for coordinating the organization's Enterprise Risk Management (ERM) approach. Answer: C is incorrect. The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise responsible for the information technology and computer systems that support enterprise goals. The CIO plays the role of a leader and reports to the chief executive officer, chief operations officer, or chief financial officer. In military organizations, they report to the commanding officer.

NEW QUESTION: 37
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. Under which of the following controls does audit control come?
A. Reactive controls
B. Detective controls
C. Protective controls
D. Preventive controls
Answer: (SHOW ANSWER)
Audit trail or audit log comes under detective controls. 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. Answer C and D are incorrect. Protective or preventative controls serve to proactively define and possibly enforce acceptable behaviors. As an example, a set of common accounting rules are defined and must be followed by any publicly traded company. Each quarter, any particular company must publicly state its current financial standing and accounting as reflected by an application of these rules. These accounting rules and the SEC requirements serve as protective or preventative controls.

NEW QUESTION: 38
You are the project manager for a construction project. The project involves casting of a column in a very narrow space. Because of lack of space, casting it is highly dangerous. High technical skill will be required for casting that column. You decide to hire a local expert team for casting that column. Which of the following types of risk response are you following?
A. Avoidance
B. Acceptance
C. Mitigation
D. Transference
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation: According to the question, you are hiring a local expert team for casting the column. As you have transferred your risk to a third party, this is the transference risk response that you have adopted.
Transference is a strategy to mitigate negative risks or threats. In this strategy, consequences and the ownership of a risk is transferred to a third party. This strategy does not eliminate the risk but transfers responsibility of managing the risk to another party. Insurance is an example of transference. AnswerC is incorrect. Mitigation is a risk response planning technique associated with threats that seeks to reduce the probability of occurrence or impact of a risk to below an acceptable threshold. Risk mitigation involves taking early action to reduce the probability and impact of a risk occurring on the project. Adopting less complex processes, conducting more tests, or choosing a more stable supplier are examples of mitigation actions. Answer A is incorrect. Avoidance involves changing the project management plan to eliminate the threat entirely. Answer: B is incorrect. 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.

NEW QUESTION: 39
Which of the following are the basic characteristics of declarative security? Each correct answer represents a complete solution. Choose all that apply.
A. It is a container-managed security.
B. It has a runtime environment.
C. All security constraints are stated in the configuration files.
D. The security policies are applied at the deployment time.
Answer: A,B,C (LEAVE A REPLY)
The following are the basic characteristics of declarative security: In declarative security, programming is not required. All security constraints are stated in the configuration files. It is a container-managed security. The application server manages the enforcing process of security constraints. It has a runtime environment. The security policies for runtime environment are represented by the deployment descriptor. It can support different environments, such as development, testing, and production. Answer D is incorrect. It is the characteristic of programmatic security.

NEW QUESTION: 40
Frank is the project manager of the NHH Project. He is working with the project team to create a plan to document the procedures to manage risks throughout the project. This document will define how risks will be identified and quantified. It will also define how contingency plans will be implemented by the project team. What document is Frank and the NHH Project team creating in this scenario?
A. Risk management plan
B. Project plan
C. Project management plan
D. Resource management plan
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation: The risk management plan, part of the comprehensive management plan, defines how risks will be identified, analyzed, monitored and controlled, and even responded to. A Risk management plan is a document arranged by a project manager to estimate the effectiveness, predict risks, and build response plans to mitigate them. It also consists of the risk assessment matrix. Risks are built in with any project, and project managers evaluate risks repeatedly and build plans to address them. The risk management plan consists of analysis of possible risks with both high and low impacts, and the mitigation strategies to facilitate the project and avoid being derailed through which the common problems arise. Risk management plans should be timely reviewed by the project team in order to avoid having the analysis become stale and not reflective of actual potential project risks. Most critically, risk management plans include a risk strategy for

project execution. AnswerC is incorrect. The project management plan is a comprehensive plan that communicates the intent of the project for all project management knowledge areas. Answer B is incorrect. The project plan is not an official PMBOK project management plan. Answer: D is incorrect. The resource management plan defines the management of project resources, such as project team members, facilities, equipment, and contractors.

NEW QUESTION: 41
Which of the following tiers addresses risks from an information system perspective?
A. Tier 0
B. Tier 3
C. Tier 2
D. Tier 1
Answer: (SHOW ANSWER)
The information system level is the tier 3. It addresses risks from an information system perspective, and is guided by the risk decisions at tiers 1 and 2. Risk decisions at tiers 1 and 2 impact the ultimate selection and deployment of requisite safeguards. This also has an impact on the countermeasures at the information system level. The RMF primarily operates at tier3 but it can also have interactions at tiers 1 and 2. Answer A is incorrect. It is an invalid Tier description. Answer D is incorrect. The Organization Level is the Tier 1, and it addresses risks from an organizational perspective. Answer C is incorrect. The mission and business process level is the Tier 2, and it addresses risks from the mission and business process perspective.

NEW QUESTION: 42
Billy is the project manager of the HAR Project and is in month six of the project. The project is scheduled to last for 18 months. Management asks Billy how often the project team is participating in risk reassessment in this project. What should Billy tell management if he's following the best practices for risk management?
A. Project risk management happens at every milestone.
B. Project risk management has been concluded with the project planning.
C. Project risk management is scheduled for every month in the 18-month project.
D. At every status meeting the project team project risk management is an agenda item.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Risk management is an ongoing project activity. It should be an agenda item at every project status meeting. AnswerA is incorrect. Milestones are good times to do reviews, but risk management should happen frequently. Answer: C is incorrect. This answer would only be correct if the project has a status meeting just once per month in the project. Answer: B is incorrect. Risk management happens throughout the project as does project planning.

NEW QUESTION: 43

Which of the following is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention?

A. Copyright

B. Snooping

C. Utility model

D. Patent

Answer: D (LEAVE A REPLY)

A patent is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention. Answer A is incorrect. 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. Answer B is incorrect. Snooping is an activity of observing the content that appears on a computer monitor or watching what a user is typing. Snooping also occurs by using software programs to remotely monitor activity on a computer or network device. Hackers or attackers use snooping techniques and equipment such as keyloggers to monitor keystrokes, capture passwords and login information, and to intercept e-mail and other private communications. Sometimes, organizations also snoop their employees legitimately to monitor their use of organizations' computers and track Internet usage. Answer C is incorrect. A utility model is an intellectual property right to protect inventions.

NEW QUESTION: 44

Which of the following refers to a process that is used for implementing information security?

A. Classic information security model

B. Five Pillars model

C. Certification and Accreditation (C&A)

D. Information Assurance (IA)

Answer: (SHOW ANSWER)

Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The C&A process is used extensively in the U.S. Federal Government. Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. Answer D is incorrect. Information

Assurance (IA) is the practice of managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. While focused dominantly on information in digital form, the full range of IA encompasses not only digital but also analog or physical form. Information assurance as a field has grown from the practice of information security, which in turn grew out of practices and procedures of computer security. Answer A is incorrect. The classic information security model is used in the practice of Information Assurance (IA) to define assurance requirements. The classic information security model, also called the CIA Triad, addresses three attributes of information and information systems, confidentiality, integrity, and availability. This C-I-A model is extremely useful for teaching introductory and basic concepts of information security and assurance; the initials are an easy mnemonic to remember, and when properly understood, can prompt systems designers and users to address the most pressing aspects of assurance. Answer B is incorrect. The Five Pillars model is used in the practice of Information Assurance (IA) to define assurance requirements. It was promulgated by the U.S. Department of Defense (DoD) in a variety of publications, beginning with the National Information Assurance Glossary, Committee on National Security Systems Instruction CNSSI-4009. Here is the definition from that publication: "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." The Five Pillars model is sometimes criticized because authentication and non-repudiation are not attributes of information or systems; rather, they are procedures or methods useful to assure the integrity and authenticity of information, and to protect the confidentiality of the same.

NEW QUESTION: 45

Which of the following testing methods tests the system efficiency by systematically selecting the suitable and minimum set of tests that are required to effectively cover the affected changes?

A. Unit testing

B. Integration testing

C. Acceptance testing

D. Regression testing

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation: Regression testing focuses on finding defects after a major code change has occurred.

Specifically, it seeks to uncover software regressions, or old bugs that have come back. Such regressions occur whenever software functionality that was previously working correctly stops working as intended.

Typically, regressions occur as an unintended consequence of program changes, when the newly developed part of the software collides with the previously existing code. Regression testing tests the system efficiency by systematically selecting the suitable and minimum set of tests that are required to effectively cover the affected changes. Answer: A is incorrect. Unit testing is a type of

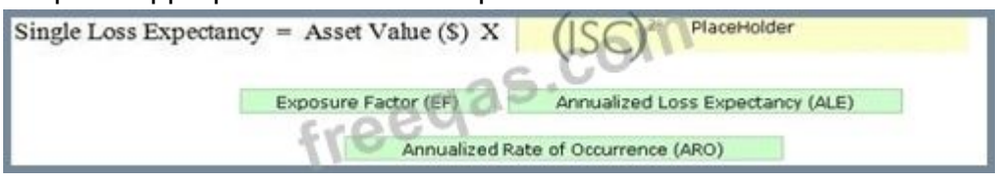
testing in which each independent unit of an application is tested separately. During unit testing, a developer takes the smallest unit of an application, isolates it from the rest of the application code, and tests it to determine whether it works as expected. Unit testing is performed before integrating these independent units into modules. The most common approach to unit testing requires drivers and stubs to be written. Drivers and stubs are programs. A driver simulates a calling unit, and a stub simulates a called unit. Answer: C is incorrect.
Acceptance testing is performed on the application before its implementation into the production environment. It is done either by a client or an application specialist to ensure that the software meets the requirement for which it was made. Answer: B is incorrect. Integration testing is a software testing that seeks to verify the interfaces between components against a software design. Software components may be integrated in an iterative way or all together ("big bang"). Normally the former is considered a better practice since it allows interface issues to be localized more quickly and fixed. Integration testing works to expose defects in the interfaces and interaction between the integrated components (modules).
Progressively larger groups of tested software components corresponding to elements of the architectural design are integrated and tested until the software works as a system.

NEW QUESTION: 46
Which of the following methods determines the principle name of the current user and returns the jav a.security.Principal object in the HttpServletRequest interface?
A. getUserPrincipal()
B. isUserInRole()
C. getRemoteUser()
D. getCallerPrincipal()
Answer: (SHOW ANSWER)
The getUserPrincipal() method determines the principle name of the current user and returns the java.security.Principal object. The java.security.Principal object contains the remote user name. The value of the getUserPrincipal() method returns null if no user is authenticated. Answer C is incorrect. The getRemoteUser() method returns the user name that is used for the client authentication. The value of the getRemoteUser() method returns null if no user is authenticated. Answer B is incorrect. The isUserInRole() method determines whether the remote user is granted a specified user role. The value of the isUserInRole() method returns true if the remote user is granted the specified user role; otherwise it returns false. Answer D is incorrect. The getCallerPrincipal() method is used to identify a caller using a java.security.Principal object. It is not used in the HttpServletRequest interface.

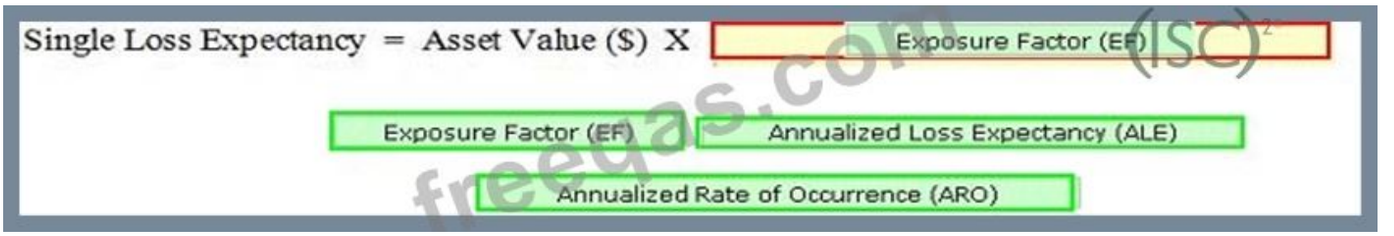
NEW QUESTION: 47

DRAG DROP

Drop the appropriate value to complete the formula.



Answer:



Explanation:

A Single Loss Expectancy (SLE) is the value in dollar ($) that is assigned to a single event. The SLE can be calculated by the following formula: SLE = Asset Value ($) X Exposure Factor (EF) The Exposure Factor (EF) represents the % of assets loss caused by a threat. The EF is required to calculate the Single Loss Expectancy (SLE). The Annualized Loss Expectancy (ALE) 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.

NEW QUESTION: 48

"Enhancing the Development Life Cycle to Produce Secure Software" summarizes the tools and practices that are helpful in producing secure software. What are these tools and practices? Each correct answer represents a complete solution. Choose three.

A. Leverage attack patterns

B. Compiler security checking and enforcement

C. Tools to detect memory violations

D. Safe software libraries
E. Code for reuse and maintainability
Answer: B,C,D (LEAVE A REPLY)
Explanation/Reference:
Explanation: The tools and practices that are helpful in producing secure software are summarized in the report "Enhancing the Development Life Cycle to Produce Secure Software". The tools and practices are as follows: Compiler security checking and enforcement Safe software libraries Runtime error checking and safety enforcement Tools to detect memory violations Code obfuscation AnswerA and E are incorrect. These are secure coding principles and practices of defensive coding.

NEW QUESTION: 49
Which of the following refers to the ability to ensure that the data is not modified or tampered with?
A. Integrity
B. Availability
C. Non-repudiation
D. Confidentiality
Answer: (SHOW ANSWER)
Integrity refers to the ability to ensure that the data is not modified or tampered with. Integrity means that data cannot be modified without authorization. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a Web site, when someone is able to cast a very large number of votes in an online poll, and so on. Answer D is incorrect. Confidentiality is the property of preventing disclosure of information to unauthorized individuals or systems. Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Answer B is incorrect. Availability means that data must be available whenever it is needed. Answer C is incorrect. Non-repudiation is the concept of ensuring that a party in a dispute cannot refuse to acknowledge, or refute the validity of a statement or contract. As a service, it provides proof of the integrity and origin of data. Although this concept can be applied to any transmission, including television and radio, by far the most common application is in the verification and trust of signatures.

NEW QUESTION: 50
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
Answer: A,B,D (LEAVE A REPLY)
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.

NEW QUESTION: 51
Which of the following roles is also known as the accreditor?
A. Data owner
B. Chief Risk Officer
C. Chief Information Officer
D. Designated Approving Authority
Answer: D (LEAVE A REPLY)
Designated Approving Authority (DAA) is also known as the accreditor. Answer A is incorrect. The data owner (information owner) is usually a member of management, in charge of a specific business unit, and is ultimately responsible for the protection and use of a specific subset of information. Answer B is incorrect. A Chief Risk Officer (CRO) is also known as Chief Risk Management Officer (CRMO). The Chief Risk Officer or Chief Risk Management Officer of a corporation is the executive accountable for enabling the efficient and effective governance of significant risks, and related opportunities, to a business and its various segments. Risks are commonly categorized as strategic, reputational, operational, financial, or compliance-related. CRO's are accountable to the Executive Committee and The Board for enabling the business to balance risk and reward. In more complex organizations, they are generally responsible for coordinating the organization's Enterprise Risk Management (ERM) approach. Answer C is incorrect. The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise responsible for the information technology and computer systems that support enterprise goals. The CIO plays the role of a leader and reports to the chief executive officer, chief operations officer, or chief financial officer. In military organizations, they report to the commanding officer.

NEW QUESTION: 52
Which of the following are the common roles with regard to data in an information classification program? Each correct answer represents a complete solution. Choose all that apply.
A. Editor
B. Custodian

C. Owner
D. User
E. Security auditor
Answer: (SHOW ANSWER)
The following are the common roles with regard to data in an information classification program: Owner Custodian User Security auditor The following are the responsibilities of the owner with regard to data in an information classification program: Determining what level of classification the information requires. Reviewing the classification assignments at regular time intervals and making changes as the business needs change. Delegating the responsibility of the data protection duties to the custodian. The following are the responsibilities of the custodian with regard to data in an information classification program: Running regular backups and routinely testing the validity of the backup data Performing data restoration from the backups when necessary Controlling access, adding and removing privileges for individual users The users must comply with the requirements laid out in policies and procedures. They must also exercise due care. A security auditor examines an organization's security procedures and mechanisms.

NEW QUESTION: 53
The Systems Development Life Cycle (SDLC) is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems. Which of the following are the different phases of system development life cycle? Each correct answer represents a complete solution.
Choose all that apply.
A. Testing
B. Implementation
C. Operation/maintenance
D. Development/acquisition
E. Disposal
F. Initiation
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: The Systems Development Life Cycle (SDLC), or Software Development Life Cycle in systems engineering, information systems, and software engineering, is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems. The concept generally refers to computers or information systems. The following are the five phases in a generic System Development Life Cycle: 1.Initiation 2.Development/acquisition 3.Implementation 4.Operation/ maintenance 5.Disposal

NEW QUESTION: 54
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 (LEAVE A REPLY)

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.

NEW QUESTION: 55

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

Answer: D (LEAVE A REPLY)

The Phase 3 of DITSCAP C&A 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 C&A level of effort, identify the main C&A 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.

NEW QUESTION: 56

Security controls are safeguards or countermeasures to avoid, counteract, or minimize security risks.

Which of the following are types of security controls? Each correct answer represents a complete solution.

Choose all that apply.

A. Common controls

B. Hybrid controls

C. Storage controls
D. System-specific controls
Answer: A,B,D (LEAVE A REPLY)
Explanation/Reference:
Explanation: Security controls are safeguards or countermeasures to avoid, counteract, or minimize security risks. The following are the types of security controls for information systems, that can be employed by an organization: 1.System-specific controls: These types of security controls provide security capability for a particular information system only. 2.Common controls: These types of security controls provide security capability for multiple information systems. 3.Hybrid controls: These types of security controls have features of both system-specific and common controls. AnswerC is incorrect. It is an invalid control.

NEW QUESTION: 57
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
Answer: B (LEAVE A REPLY)
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.

NEW QUESTION: 58
Which of the following documents were developed by NIST for conducting Certification & Accreditation (C&A)? Each correct answer represents a complete solution. Choose all that apply.
A. NIST Special Publication 800-60
B. NIST Special Publication 800-53
C. NIST Special Publication 800-37A
D. NIST Special Publication 800-59
E. NIST Special Publication 800-37
F. NIST Special Publication 800-53A
Answer: A,B,D,E,F (LEAVE A REPLY)
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. Answer C is incorrect. There is no such type of NIST document.

NEW QUESTION: 59
What NIACAP certification levels are recommended by the certifier? Each correct answer represents a complete solution. Choose all that apply.
A. Comprehensive Analysis
B. Maximum Analysis
C. Detailed Analysis
D. Minimum Analysis
E. Basic Security Review
F. Basic System Review
Answer: A,C,D,E (LEAVE A REPLY)
Explanation/Reference:
Explanation: NIACAP has four levels of certification. These levels ensure that the appropriate C&A are performed for varying schedule and budget limitations. The certifier must analyze the system's business functions. The certifier determines the degree of confidentiality, integrity, availability, and accountability, and then recommends one of the following NIACAP certification levels: Level 1 - Basic Security Review Level 2 - Minimum Analysis Level 3 - Detailed Analysis Level 4 - Comprehensive Analysis AnswerB and F are incorrect. No such types of levels exist.

NEW QUESTION: 60
You are responsible for network and information security at a metropolitan police station. The most important concern is that unauthorized parties are not able to access data. What is this called?
A. Confidentiality
B. Availability
C. Integrity
D. Encryption
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation: The CIA (Confidentiality, Integrity, and Availability) triangle is concerned with three facets of security. Confidentiality is the concern that data be secure from unauthorized access. AnswerB and C are incorrect. The CIA (Confidentiality, Integrity, and Availability) triangle is concerned with three facets of security. Integrity is the concern that data not be altered without it being traceable. Availability is the concern that the data, while being secured, is readily

accessible. AnswerD is incorrect. Confidentiality may be implemented with encryption but encryption is just a technique to obtain confidentiality.

NEW QUESTION: 61
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
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 62
Which of the following phases of the DITSCAP C&A process is used to define the C&A level of effort, to identify the main C&A 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
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: The Phase 1 of the DITSCAP C&A process is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. AnswerC is incorrect. The Phase 2 of the DITSCAP C&A process is known as Verification. Answer: D is incorrect. The Phase 3 of the DITSCAP C&A process is known as Validation. Answer: B is incorrect. The Phase 4 of the DITSCAP C&A process is known as Post Accreditation.

NEW QUESTION: 63
Shoulder surfing is a type of in-person attack in which the attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard of an employee's computer while he is typing in his password at any access point such as a terminal/Web site.
Which of the following is violated in a shoulder surfing attack?
A. Integrity
B. Availability
C. Confidentiality
D. Authenticity
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: Confidentiality is violated in a shoulder surfing attack. The CIA triad provides the following three tenets for which security practices are measured: Confidentiality: It is the property of preventing disclosure of information to unauthorized individuals or systems. Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality.
Integrity: It means that data cannot be modified without authorization. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on. Availability: It means that data must be available at every time when it is needed. AnswerD is incorrect. Authenticity is not a tenet of the CIA triad.

NEW QUESTION: 64

You are the project manager for GHY Project and are working to create a risk response for a negative risk.
You and the project team have identified the risk that the project may not complete on time, as required by the management, due to the creation of the user guide for the software you're creating. You have elected to hire an external writer in order to satisfy the requirements and to alleviate the risk event. What type of risk response have you elected to use in this instance?
A. Transference
B. Exploiting
C. Avoidance
D. Sharing
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation: This is an example of transference as you have transferred the risk to a third party. Transference almost always is done with a negative risk event and it usually requires a contractual relationship.

NEW QUESTION: 65
Mark works as a Network Administrator for NetTech Inc. The company has a Windows 2000 domain-based network. Users report that they are unable to log on to the network. Mark finds that accounts are locked out due to multiple incorrect log on attempts. What is the most likely cause of the account lockouts?
A. Spoofing
B. Brute force attack
C. SYN attack
D. PING attack
Answer: B (LEAVE A REPLY)
Brute force attack is the most likely cause of the account lockouts. In a brute force attack, unauthorized users attempt to log on to a network or a computer by using multiple possible user names and passwords. Windows 2000 and other network operating systems have a security feature that locks a user account if the number of failed logon attempts occur within a specified period of time, based on the security policy lockout settings. Answer A 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 C is incorrect. A SYN attack affects computers running on the TCP/IP protocol. It is a protocol-level attack that can render a computer's network services unavailable. A SYN attack is also known as SYN flooding. Answer D is incorrect. When a computer repeatedly sends ICMP echo requests to another computer, it is known as a PING attack.

NEW QUESTION: 66
SIMULATION
Fill in the blank with an appropriate phrase The is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity.
Answer:
Biba model
Explanation/Reference:
Explanation: 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.

NEW QUESTION: 67
Which of the following software review processes increases the software security by removing the common vulnerabilities, such as format string exploits, race conditions, memory leaks, and buffer overflows?
A. Management review
B. Code review
C. Peer review
D. Software audit review
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: A code review is a systematic examination of computer source code, which searches and resolves issues occurred in the initial development phase. It increases the software security by removing common vulnerabilities, such as format string exploits, race conditions, memory leaks, and buffer overflows. A code review is performed in the following forms: Pair programming Informal walkthrough Formal inspection Answer: C is incorrect. A peer review is an examination process in which author and one or more colleagues examine a work product, such as document, code, etc., and evaluate technical content and quality. According to the Capability Maturity Model, peer review offers a systematic engineering practice in order to detect and resolve issues occurring in the software artifacts, and stops the leakage into field operations. Answer: A is incorrect. Management review is a management study into a project's status and allocation of resources. Answer: D is incorrect. In software audit review one or more auditors, who are not members of the software development organization, perform an independent examination of a software product, software process, or a set of software processes for assessing compliance with specifications, standards, contractual agreements, or other specifications.

NEW QUESTION: 68
The Software Configuration Management (SCM) process defines the need to trace changes, and the ability to verify that the final delivered software has all of the planned enhancements that are

supposed to be included in the release. What are the procedures that must be defined for each software project to ensure that a sound SCM process is implemented? Each correct answer represents a complete solution. Choose all that apply.

A. Configuration status accounting

B. Configuration change control

C. Configuration identification

D. Configuration audits

E. Configuration implementation

F. Configuration deployment

Answer: A,B,C,D (LEAVE A REPLY)

The SCM process defines the need to trace changes, and the ability to verify that the final delivered software has all of the planned enhancements that are supposed to be included in the release. It identifies four procedures that must be defined for each software project to ensure that a sound SCM process is implemented. They are as follows: 1.Configuration identification: 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. 2.Configuration change control: Configuration change control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them. 3.Configuration status accounting: Configuration status accounting is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time. 4.Configuration audits: 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.

NEW QUESTION: 69

FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls have been implemented?

A. Level 2

B. Level 3

C. Level 5

D. Level 1

E. Level 4

Answer: B (LEAVE A REPLY)

The following are the five levels of FITSAF based on SEI's Capability Maturity Model (CMM): Level 1: The first level reflects that an asset has documented a security policy. Level 2: The second level shows that the asset has documented procedures and controls to implement the policy. Level 3: The third level indicates that these procedures and controls have been

implemented. Level 4: The fourth level shows that the procedures and controls are tested and reviewed. Level 5: The fifth level is the final level and shows that the asset has procedures and controls fully integrated into a comprehensive program.

NEW QUESTION: 70
In which of the following cryptographic attacking techniques does an attacker obtain encrypted messages that have been encrypted using the same encryption algorithm?
A. Chosen plaintext attack
B. Chosen ciphertext attack
C. Ciphertext only attack
D. Known plaintext attack
Answer: (SHOW ANSWER)
In a ciphertext only attack, an attacker obtains encrypted messages that have been encrypted using the same encryption algorithm.

NEW QUESTION: 71
The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum standard process for the certification and accreditation of computer and telecommunications systems that handle U.S. national security information. What are the different types of NIACAP accreditation? Each correct answer represents a complete solution. Choose all that apply.
A. Site accreditation
B. Type accreditation
C. Secure accreditation
D. System accreditation
Answer: A,B,D (LEAVE A REPLY)
NIACAP accreditation is of three types depending on what is being certified. They are as follows: 1.Site accreditation: This type of accreditation evaluates the applications and systems at a specific, self contained location. 2.Type accreditation: This type of accreditation evaluates an application or system that is distributed to a number of different locations. 3.System accreditation: This accreditation evaluates a major application or general support system. Answer C is incorrect. No such type of NIACAP accreditation exists.

NEW QUESTION: 72
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
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation: 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. AnswerC 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.

NEW QUESTION: 73
"Enhancing the Development Life Cycle to Produce Secure Software" summarizes the tools and practices that are helpful in producing secure software. What are these tools and practices? Each correct answer represents a complete solution. Choose three.
A. Leverage attack patterns
B. Compiler security checking and enforcement
C. Tools to detect memory violations
D. Safe software libraries
E. Code for reuse and maintainability
Answer: (SHOW ANSWER)
The tools and practices that are helpful in producing secure software are summarized in the report "Enhancing the Development Life Cycle to Produce Secure Software". The tools and practices are as follows: Compiler security checking and enforcement Safe software libraries Runtime error checking and safety enforcement Tools to detect memory violations Code obfuscation Answer A and E are incorrect. These are secure coding principles and practices of defensive coding.

NEW QUESTION: 74

Which of the following DoD directives defines DITSCAP as the standard C&A process for the Department of Defense?

A. DoD 8910.1

B. DoD 5200.22-M

C. DoD 8000.1

D. DoD 5200.40

Answer: D (LEAVE A REPLY)

DITSCAP stands for DoD Information Technology Security Certification and Accreditation Process. The DoD Directive 5200.40 (DoD Information Technology Security Certification and Accreditation Process) established the DITSCAP as the standard C&A process for the Department of Defense. 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, in 2006. Answer B is incorrect. This DoD Directive is known as National Industrial Security Program Operating Manual. Answer C is incorrect. This DoD Directive is known as Defense Information Management (IM) Program. Answer A is incorrect. This DoD Directive is known as Management and Control of Information Requirements.

NEW QUESTION: 75

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully performed the following steps of the pre-attack phase to check the security of the We-are-secure network: Gathering information Determining the network range Identifying active systems Now, he wants to find the open ports and applications running on the network.

Which of the following tools will he use to accomplish his task?

A. ARIN

B. APNIC

C. RIPE

D. SuperScan

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation: In such a situation, John will use the SuperScan tool to find the open ports and applications on the We-are-secure network. SuperScan is a TCP/UDP port scanner. It also works as a ping sweeper and hostname resolver. It can ping a given range of IP addresses and resolve the host name of the remote system. The features of SuperScan are as follows: It scans any port range from a built-in list or any given range. It performs ping scans and port scans using any IP range. It modifies the port list and port descriptions using the built in editor. It connects to any discovered open port using user-specified "helper" applications. It has the transmission speed control utility. AnswerC, A, and B are incorrect. RIPE, ARIN, and APNIC are the Regional Internet Registries (RIR) that manage, distribute, and register public IP addresses within their respective regions. These can be used as passive tools by an attacker to determine the network range.

NEW QUESTION: 76
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
Answer: A,B,D (LEAVE A REPLY)
Explanation/Reference:
Explanation: 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 AnswerC is incorrect.
System classification is not one of the objectives of a security program.

NEW QUESTION: 77
Which of the following security objectives are defined for information and information systems by the FISMA? Each correct answer represents a part of the solution. Choose all that apply.
A. Authenticity
B. Availability
C. Integrity
D. Confidentiality
Answer: B,C,D (LEAVE A REPLY)
FISMA defines the following three security objectives for information and information systems: Confidentiality: It means that the data should only be accessible to authorized users. Access includes printing, displaying, and other such forms of disclosure, including simply revealing the existence of an object. Integrity: It means that only authorized users are able to modify data.

Modification admits changing, changing the status, deleting, and creating. Availability: It means that the data should only be available to authorized users. Answer A is incorrect. Authenticity is not defined by the FISMA as one of the security objectives for information and information systems.

NEW QUESTION: 78
Which of the following features of SIEM products is used in analysis for identifying potential problems and reviewing all available data that are associated with the problems?
A. Security knowledge base
B. Graphical user interface
C. Asset information storage and correlation
D. Incident tracking and reporting
Answer: B (LEAVE A REPLY)
SIEM product has a graphical user interface (GUI) which is used in analysis for identifying potential problems and reviewing all available data that are associated with the problems. A graphical user interface (GUI) is a type of user interface that allows people to interact with programs in more ways than typing commands on computers. The term came into existence because the first interactive user interfaces to computers were not graphical; they were text- and-keyboard oriented and usually consisted of commands a user had to remember and computer responses that were infamously brief. A GUI offers graphical icons, and visual indicators, as opposed to text-based interfaces, typed command labels or text navigation to fully represent the information and actions available to a user. The actions are usually performed through direct manipulation of the graphical elements.

NEW QUESTION: 79
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He finds that the We-are-secure server is vulnerable to attacks. As a countermeasure, he suggests that the Network Administrator should remove the IPP printing capability from the server. He is suggesting this as a countermeasure against _____.
A. SNMP enumeration
B. IIS buffer overflow
C. NetBIOS NULL session
D. DNS zone transfer
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: Removing the IPP printing capability from a server is a good countermeasure against an IIS buffer overflow attack. A Network Administrator should take the following steps to prevent a Web server from IIS buffer overflow attacks: Conduct frequent scans for server vulnerabilities. Install the upgrades of Microsoft service packs.

Implement effective firewalls. Apply URLScan and IISLockdown utilities. Remove the IPP printing capability. AnswerD is incorrect. The following are the DNS zone transfer countermeasures: Do not allow DNS zone transfer using the DNS property sheet: a.Open DNS. b.Right-click a DNS zone and click Properties. c.On the Zone Transfer tab, clear the Allow zone transfers check box. Configure the master DNS server to allow zone transfers only from secondary DNS servers: a.Open DNS. b.Right-click a DNS zone and click Properties. c.On the zone transfer tab, select the Allow zone transfers check box, and then do one of the following: To allow zone transfers only to the DNS servers listed on the name servers tab, click on the Only to the servers listed on the Name Server tab. To allow zone transfers only to specific DNS servers, click Only to the following servers, and add the IP address of one or more servers. Deny all unauthorized inbound connections to TCP port 53. Implement DNS keys and encrypted DNS payloads.
AnswerA is incorrect. The following are the countermeasures against SNMP enumeration: 1.Removing
the SNMP agent or disabling the SNMP service 2.Changing the default PUBLIC community name when
'shutting off SNMP' is not an option 3.Implementing the Group Policy security option called Additional restrictions for anonymous connections 4.Restricting access to NULL session pipes and NULL session shares 5.Upgrading SNMP Version 1 with the latest version 6.Implementing Access control list filtering to allow only access to the read-write community from approved stations or subnets AnswerC is incorrect.
NetBIOS NULL session vulnerabilities are hard to prevent, especially if NetBIOS is needed as part of the infrastructure. One or more of the following steps can be taken to limit NetBIOS NULL session vulnerabilities: 1.Null sessions require access to the TCP 139 or TCP 445 port, which can be disabled by a Network Administrator. 2.A Network Administrator can also disable SMB services entirely on individual hosts by unbinding WINS Client TCP/IP from the interface. 3.A Network Administrator can also restrict the anonymous user by editing the registry values: a.Open regedit32, and go to HKLM\SYSTEM
\CurrentControlSet\LSA. b.Choose edit > add value. Value name: RestrictAnonymous Data Type: REG_WORD Value: 2

NEW QUESTION: 80
Which of the following activities are performed by the 'Do' cycle component of PDCA (plan-do-check-act)?
Each correct answer represents a complete solution. Choose all that apply.
A. It detects and responds to incidents properly.
B. It determines controls and their objectives.
C. It manages resources that are required to achieve a goal.
D. It performs security awareness training.
E. It operates the selected controls.
Answer: A,C,D,E (LEAVE A REPLY)
Explanation/Reference:

Explanation: The 'Do' cycle component performs the following activities: It operates the selected controls. It detects and responds to incidents properly. It performs security awareness training. It manages resources that are required to achieve a goal. AnswerB is incorrect. This activity is performed by the 'Plan' cycle component of PDCA.

NEW QUESTION: 81
Which of the following actions does the Data Loss Prevention (DLP) technology take when an agent detects a policy violation for data of all states? Each correct answer represents a complete solution. Choose all that apply.
A. It creates an alert.
B. It quarantines the file to a secure location.
C. It reconstructs the session.
D. It blocks the transmission of content.
Answer: (SHOW ANSWER)
When an agent detects a policy violation for data of all states, the Data Loss prevention (DLP) technology takes one of the following actions: It creates an alert. It notifies an administrator of a violation. It quarantines the file to a secure location. It encrypts the file. It blocks the transmission of content. Answer C is incorrect. Data Loss Prevention (DLP) reconstructs the session when data is in motion.

NEW QUESTION: 82
The organization level is the Tier 1 and it addresses risks from an organizational perspective. What are the various Tier 1 activities? Each correct answer represents a complete solution. Choose all that apply.
A. The organization plans to use the degree and type of oversight, to ensure that the risk management strategy is being effectively carried out.
B. The level of risk tolerance.
C. The techniques and methodologies an organization plans to employ, to evaluate information system- related security risks.
D. The RMF primarily operates at Tier 1.
Answer: A,B,C (LEAVE A REPLY)
Explanation/Reference:
Explanation: The Organization Level is the Tier 1, and it addresses risks from an organizational perspective. It includes the following points: The techniques and methodologies an organization plans to employ, to evaluate information system-related security risks. During risk assessment, the methods and procedures the organization plans to use, to evaluate the significance of the risks identified. The types and extent of risk mitigation measures the organization plans to employ, to address identified risks. The level of risk tolerance. According to the environment of operation, how the organization plans to monitor risks on an ongoing basis, given the inevitable changes to organizational information system.

The organization plans to use the degree and type of oversight, in order to ensure that the risk management strategy is being effectively carried out.Answer: D is incorrect. The RMF primarily operates at Tier 3.

NEW QUESTION: 83
You work as a project manager for BlueWell Inc. You are working on a project and the management wants a rapid and cost-effective means for establishing priorities for planning risk responses in your project. Which risk management process can satisfy management's objective for your project?
A. Qualitative risk analysis
B. Historical information
C. Rolling wave planning
D. Quantitative analysis
Answer: (SHOW ANSWER)
Qualitative risk analysis is the best answer as it is a fast and low-cost approach to analyze the risk impact and its effect. It can promote certain risks onto risk response planning. Qualitative Risk Analysis uses the likelihood and impact of the identified risks in a fast and cost-effective manner. Qualitative Risk Analysis establishes a basis for a focused quantitative analysis or Risk Response Plan by evaluating the precedence of risks with a concern to impact on the project's scope, cost, schedule, and quality objectives. The qualitative risk analysis is conducted at any point in a project life cycle. The primary goal of qualitative risk analysis is to determine proportion of effect and theoretical response. The inputs to the Qualitative Risk Analysis process are: Organizational process assets Project Scope Statement Risk Management Plan Risk Register Answer B is incorrect. Historical information can be helpful in the qualitative risk analysis, but it is not the best answer for the question as historical information is not always available (consider new projects). Answer D is incorrect. Quantitative risk analysis is in-depth and often requires a schedule and budget for the analysis. Answer C is incorrect. Rolling wave planning is not a valid answer for risk analysis processes.

NEW QUESTION: 84
Which of the following secure coding principles and practices defines the appearance of code listing so that a code reviewer and maintainer who have not written that code can easily understand it?
A. Make code forward and backward traceable
B. Review code during and after coding
C. Use a consistent coding style
D. Keep code simple and small
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: Use a consistent coding style is one of the principles and practices that contribute to defensive coding. This principle defines the appearance of code listing so that a code reviewer

and maintainer who have not written that code can easily understand it. For this purpose, all programmers of a team must follow the same guidelines. Answer: D is incorrect. Keep code simple and small defines that it is easy to verify the software security when a programmer uses small and simple code base. Answer: A is incorrect. Make code forward and backward traceable defines that traceability is necessary in order to validate requirements, prevent defects, and find and solve inconsistencies among all objects generated in the SDLC phases. Answer: B is incorrect. Review code during and after coding defines that code must be examined in order to identify coding errors in modules.

NEW QUESTION: 85
Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?
A. Single Loss Expectancy (SLE)
B. Annualized Rate of Occurrence (ARO)
C. Safeguard
D. Exposure Factor (EF)
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: The Annualized Rate of Occurrence (ARO) is a number that represents the estimated frequency at 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. AnswerD is incorrect. The Exposure Factor (EF) represents the % of assets loss caused by a threat. The EF is required to calculate the Single Loss Expectancy (SLE). Answer: A is incorrect. The Single Loss Expectancy (SLE) is the value in dollars that is assigned to a single event. SLE = Asset Value ($) X Exposure Factor (EF) Answer: C is incorrect. Safeguard acts as a countermeasure for reducing the risk associated with a specific threat or a group of threats.

NEW QUESTION: 86
What are the subordinate tasks of the Initiate and Plan IA C&A phase of the DIACAP process? Each correct answer represents a complete solution. Choose all that apply.
A. Initiate IA implementation plan
B. Develop DIACAP strategy
C. Assign IA controls.
D. Assemble DIACAP team
E. Register system with DoD Component IA Program.
F. Conduct validation activity.
Answer: (SHOW ANSWER)
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. The subordinate tasks of the Initiate and Plan IA C&A phase are as follows: Register system with DoD Component IA Program. Assign IA controls. Assemble DIACAP team. Develop DIACAP

strategy. Initiate IA implementation plan. Answer F is incorrect. Validation activities are conducted in the second phase of the DIACAP process, i.e., Implement and Validate Assigned IA Controls.

NEW QUESTION: 87
What are the subordinate tasks of the Implement and Validate Assigned IA Control phase in the DIACAP process? Each correct answer represents a complete solution. Choose all that apply.
A. Conduct validation activities.
B. Execute and update IA implementation plan.
C. Combine validation results in DIACAP scorecard.
D. Conduct activities related to the disposition of the system data and objects.
Answer: A,B,C (LEAVE A REPLY)
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. The subordinate tasks of the Implement and Validate Assigned IA Control phase in the DIACAP process are as follows: Execute and update IA implementation plan. Conduct validation activities. Combine validation results in the DIACAP scorecard. Answer D is incorrect. The activities related to the disposition of the system data and objects are conducted in the fifth phase of the DIACAP process. The fifth phase of the DIACAP process is known as Decommission System.

NEW QUESTION: 88
FIPS 199 defines the three levels of potential impact on organizations. Which of the following potential impact levels shows limited adverse effects on organizational operations, organizational assets, or individuals?
A. Moderate
B. Low
C. Medium
D. High
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: The potential impact is called low if the loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Answer: C is incorrect. Such a type of potential impact level does not exist Answer: A is incorrect. The potential impact is known to be moderate if the loss of confidentiality, integrity, or availability is expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Answer: D is incorrect. The potential impact is called high if the loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

NEW QUESTION: 89

Which of the following ISO standards provides guidelines for accreditation of an organization that is concerned with certification and registration related to ISMS?

A. ISO 27006

B. ISO 27005

C. ISO 27003

D. ISO 27004

Answer: (SHOW ANSWER)

ISO 27006 is an information security standard developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is entitled as "Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems". The ISO 27006 standard provides guidelines for accreditation of an organization which is concerned with certification and registration related to ISMS. The ISO 27006 standard contains the following elements: Scope Normative references Terms and definitions Principles General requirements Structural requirements Resource requirements Information requirements Process requirements Management system requirements for certification bodies Information security risk communication Information security risk monitoring and review Annex A.

Defining the scope of process Annex B.

Asset valuation and impact assessment Annex C.

Examples of typical threats Annex D.

Vulnerabilities and vulnerability assessment methods Annex E.

Information security risk assessment (ISRA) approaches Answer C is incorrect.

The ISO 27003 standard provides guidelines for implementing an ISMS (Information Security Management System).

Answer D is incorrect. The ISO 27004 standard provides guidelines on specifications and use of measurement techniques for the assessment of the effectiveness of an implemented information security management system and controls. Answer B is incorrect. The ISO 27005 standard provides guidelines for information security risk management.

NEW QUESTION: 90

You work as a project manager for BlueWell Inc. You are working on a project and the management wants a rapid and cost-effective means for establishing priorities for planning risk responses in your project.

Which risk management process can satisfy management's objective for your project?

A. Qualitative risk analysis

B. Historical information

C. Rolling wave planning

D. Quantitative analysis

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation: Qualitative risk analysis is the best answer as it is a fast and low-cost approach to analyze the risk impact and its effect. It can promote certain risks onto risk response planning. Qualitative Risk Analysis uses the likelihood and impact of the identified risks in a fast and cost-effective manner. Qualitative Risk Analysis establishes a basis for a focused quantitative analysis or Risk Response Plan by evaluating the precedence of risks with a concern to impact on the project's scope, cost, schedule, and quality objectives.
The qualitative risk analysis is conducted at any point in a project life cycle. The primary goal of qualitative risk analysis is to determine proportion of effect and theoretical response. The inputs to the Qualitative Risk Analysis process are: Organizational process assets Project Scope Statement Risk Management Plan Risk Register Answer: B is incorrect. Historical information can be helpful in the qualitative risk analysis, but it is not the best answer for the question as historical information is not always available (consider new projects). Answer: D is incorrect. Quantitative risk analysis is in-depth and often requires a schedule and budget for the analysis. Answer: C is incorrect. Rolling wave planning is not a valid answer for risk analysis processes.

NEW QUESTION: 91
Which of the following persons in an organization is responsible for rejecting or accepting the residual risk for a system?
A. Information Systems Security Officer (ISSO)
B. Designated Approving Authority (DAA)
C. System Owner
D. Chief Information Security Officer (CISO)
Answer: (SHOW ANSWER)
The authorizing official is the senior manager responsible for approving the working of the information system. He is responsible for the risks of operating the information system within a known environment through the security accreditation phase. In many organizations, the authorizing official is also referred as approving/accrediting authority (DAA) or the Principal Approving Authority (PAA). Answer C is incorrect. The system owner has the responsibility of informing the key officials within the organization of the requirements for a security C&A of the information system. He makes the resources available, and provides the relevant documents to support the process. Answer A 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 & Accreditation (C&A). 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 & Accreditation (C&A) packages. Answer D is incorrect. The CISO has the responsibility of carrying out the CIO's FISMA responsibilities. He manages the information security program functions.

NEW QUESTION: 92
The DARPA paper defines various procedural patterns to perform secure system development practices.
Which of the following patterns does it include? Each correct answer represents a complete solution.
Choose three.
A. Hidden implementation
B. Document the server configuration
C. Patch proactively
D. Red team the design
E. Password propagation
Answer: B,C,D (LEAVE A REPLY)
Explanation/Reference:
Explanation: The following procedural patterns are defined by the DARPA paper in order to perform secure software development practices: Build the server from the ground up: It includes the following features:
Build the server from the ground up. Identify the default installation of the operating system and applications. Support hardening procedures to remove unnecessary services. Identify a vulnerable service for ongoing risk management. Choose the right stuff: It defines guidelines to select right commercial off- the-shelf (COTS) components and decide whether to use and build custom components. Document the server configuration: It supports the creation of an initial configuration baseline and tracks all modifications made to servers and application configurations. Patch proactively: It supports in applying patches as soon as they are available rather than waiting until the systems cooperate. Red team the design: It supports an independent security assessment from the perspective of an attacker in the quality assurance or testing stage. An independent security assessment is helpful in addressing a security issue before it occurs.
AnswerA is incorrect. Hidden implementation pattern is not defined in the DARPA paper. This pattern is applicable to software assurance in general.
Hidden implementation limits the ability of an attacker to distinguish the internal workings of an application.
AnswerE is incorrect. Password propagation is not defined in the DARPA paper. This pattern is applicable

to aspects of authentication in a Web application. Password propagation provides an alternative by requiring that a user's authentication credentials be verified by the database before providing access to that user's data.

NEW QUESTION: 93
The IAM/CA makes certification accreditation recommendations to the DAA. The DAA issues accreditation determinations. Which of the following are the accreditation determinations issued by the DAA? Each correct answer represents a complete solution. Choose all that apply.
A. IATT
B. IATO
C. DATO
D. ATO
E. ATT
Answer: A,B,C,D (LEAVE A REPLY)
The DAA issues one of the following four accreditation determinations: Approval to Operate (ATO): It is an authorization of a DoD information system to process, store, or transmit information. Interim Approval to Operate (IATO): It is a temporary approval to operate based on an assessment of the implementation status of the assigned IA Controls. Interim Approval to Test (IATT): It is a temporary approval to conduct system testing based on an assessment of the implementation status of the assigned IA Controls. Denial of Approval to Operate (DATO): It is a determination that a DoD information system cannot operate because of an inadequate IA design or failure to implement assigned IA Controls. Answer E is incorrect. No such type of accreditation determination exists.
Topic 2, Volume B

NEW QUESTION: 94
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
Answer: D (LEAVE A REPLY)
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 Generals (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.

NEW QUESTION: 95
Which of the following are the scanning methods used in penetration testing? Each correct answer represents a complete solution. Choose all that apply.
A. Vulnerability
B. Port
C. Services
D. Network
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: The vulnerability, port, and network scanning tools are used in penetration testing. Vulnerability scanning is a process in which a Penetration Tester uses various tools to assess computers, computer systems, networks or applications for weaknesses. There are a number of types of vulnerability scanners available today, distinguished from one another by a focus on particular targets. While functionality varies between different types of vulnerability scanners, they share a common, core purpose of enumerating the vulnerabilities present in one or more targets. Vulnerability scanners are a core technology component of Vulnerability management. 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. Network scanning is a penetration testing activity in which a penetration tester or an attacker identifies active hosts on a network, either to attack them or to perform security assessment. A penetration tester uses various tools to identify all the live or responding hosts on the network and their corresponding IP addresses. AnswerC is incorrect. This option comes under vulnerability scanning.

NEW QUESTION: 96
Which of the following ISO standards is entitled as "Information technology - Security techniques Information security management - Measurement"?
A. ISO 27003
B. ISO 27005
C. ISO 27004
D. ISO 27006
Answer: C (LEAVE A REPLY)
ISO 27004 is an information security standard developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is entitled as "Information technology - Security techniques - Information security management Measurement". The ISO 27004 standard provides guidelines on specifications and use of measurement techniques for the assessment of the effectiveness of an implemented information security management system and controls. It also helps an organization in establishing the effectiveness of ISMS implementation, embracing benchmarking, and performance targeting within the PDCA (plan-do-check-act) cycle. Answer A is incorrect. ISO 27003 is entitled as "Information Technology - Security techniques - Information security management system implementation guidance". Answer B is incorrect. ISO 27005 is entitled as "ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management". Answer D is incorrect. ISO 27006 is entitled as "Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems".

NEW QUESTION: 97
Which of the following are the responsibilities of a custodian with regard to data in an information classification program? Each correct answer represents a complete solution. Choose three.
A. Performing data restoration from the backups when necessary
B. Running regular backups and routinely testing the validity of the backup data
C. Determining what level of classification the information requires
D. Controlling access, adding and removing privileges for individual users

Answer: A,B,D (LEAVE A REPLY)
Explanation/Reference:
Explanation: The owner of information delegates the responsibility of protecting that information to a custodian. The following are the responsibilities of a custodian with regard to data in an information classification program: Running regular backups and routinely testing the validity of the backup data Performing data restoration from the backups when necessary Controlling access, adding and removing privileges for individual users AnswerC is incorrect. Determining what level of classification the information requires is the responsibility of the owner.

NEW QUESTION: 98
In which of the following phases of the DITSCAP process does Security Test and Evaluation (ST&E) occur?
A. Phase 2
B. Phase 4
C. Phase 3
D. Phase 1
Answer: C (LEAVE A REPLY)
Security Test and Evaluation (ST&E) occurs in Phase 3 of the DITSCAP C&A process. Answer D is incorrect. The Phase 1 of DITSCAP C&A is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. The Phase 1 starts with the input of the mission need. This phase comprises three process activities: Document mission need Registration Negotiation Answer A is incorrect. The Phase 2 of DITSCAP C&A is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. This phase takes place between the signing of the initial version of the SSAA and the formal accreditation of the system. This phase verifies security requirements during system development. The process activities of this phase are as follows: Configuring refinement of the SSAA System development Certification analysis Assessment of the Analysis Results Answer B is incorrect. 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

NEW QUESTION: 99
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 (LEAVE A REPLY)
Explanation/Reference:
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'. DoD 7950.1-M:
This DoD directive refers to the 'Defense Automation Resources Management Manual'. DoDD 8000.1: This DoD directive refers to the 'Defense Information Management (IM) Program'. DoD 8910.1: This DoD directive refers to the 'Management and Control of Information Requirements'.

NEW QUESTION: 100
Which of the following statements are true about declarative security? Each correct answer represents a complete solution. Choose all that apply.
A. It is employed in a layer that relies outside of the software code or uses attributes of the code.
B. It applies the security policies on the software applications at their runtime.
C. In this security, authentication decisions are made based on the business logic.
D. In this security, the security decisions are based on explicit statements.
Answer: A,B,D (LEAVE A REPLY)
Declarative security applies the security policies on the software applications at their runtime. In this type of security, the security decisions are based on explicit statements that confine security behavior. Declarative security applies security permissions that are required for the software application to access the local resources and provides role-based access control to an individual software component and software application. It is employed in a layer that relies outside of the software code or uses attributes of the code. Answer C is incorrect. In declarative security, authentication decisions are coarse-grained in nature from an operational or external security perspective.

NEW QUESTION: 101
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 (LEAVE A REPLY)
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.

NEW QUESTION: 102
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
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation: 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.

NEW QUESTION: 103
The Information System Security Officer (ISSO) and Information System Security Engineer (ISSE) play the role of a supporter and advisor, respectively. Which of the following statements are true about ISSO and ISSE? Each correct answer represents a complete solution. Choose all that apply.
A. An ISSE manages the security of the information system that is slated for Certification & Accreditation (C&A).
B. An ISSE provides advice on the continuous monitoring of the information system.
C. An ISSO manages the security of the information system that is slated for Certification & Accreditation (C&A).
D. An ISSE provides advice on the impacts of system changes.
E. An ISSO takes part in the development activities that are required to implement system changes.
Answer: B,C,D (LEAVE A REPLY)
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 & Accreditation (C&A). 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 & Accreditation (C&A)

packages. An Information System Security Engineer (ISSE) plays the role of an advisor. The responsibilities of an Information System Security Engineer are as follows: Provides view on the continuous monitoring of the information system. Provides advice on the impacts of system changes. Takes part in the configuration management process. Takes part in the development activities that are required to implement system changes. Follows approved system changes.

NEW QUESTION: 104
Which of the following provides an easy way to programmers for writing lower-risk applications and retrofitting security into an existing application?
A. Watermarking
B. ESAPI
C. Encryption wrapper
D. Code obfuscation
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: ESAPI (Enterprise Security API) is a group of classes that encapsulate the key security operations, needed by most of the applications. It is a free, open source, Web application security control library. ESAPI provides an easy way to programmers for writing lower-risk applications and retrofitting security into an existing application. It offers a solid foundation for new development. Answer: A is incorrect. Watermarking is the process of embedding information into software in a way that is difficult to remove. Answer: C is incorrect. Encryption wrapper dynamically encrypts and decrypts all the software code at runtime. Answer: D is incorrect. Code obfuscation is designed to protect code from decompilation.

NEW QUESTION: 105
You are responsible for network and information security at a metropolitan police station. The most important concern is that unauthorized parties are not able to access data. What is this called?
A. Confidentiality
B. Availability
C. Integrity
D. Encryption
Answer: A (LEAVE A REPLY)
The CIA (Confidentiality, Integrity, and Availability) triangle is concerned with three facets of security. Confidentiality is the concern that data be secure from unauthorized access. Answer B and C are incorrect. The CIA (Confidentiality, Integrity, and Availability) triangle is concerned with three facets of security. Integrity is the concern that data not be altered without it being traceable. Availability is the concern that the data, while being secured, is readily accessible. Answer D is incorrect. Confidentiality may be implemented with encryption but encryption is just a technique to obtain confidentiality.

NEW QUESTION: 106
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: A,B,D (LEAVE A REPLY)
Explanation/Reference:
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.

NEW QUESTION: 107
In which of the following testing methods is the test engineer equipped with the knowledge of system and designs test cases or test data based on system knowledge?
A. Integration testing
B. Regression testing
C. Whitebox testing
D. Graybox testing
Answer: D (LEAVE A REPLY)
Graybox testing is a combination of whitebox testing and blackbox testing. In graybox testing, the test engineer is equipped with the knowledge of system and designs test cases or test data based on system knowledge. The security tester typically performs graybox testing to find vulnerabilities in software and network system. Answer C is incorrect. Whitebox testing is a testing technique in which an organization provides full knowledge about the infrastructure to the testing team. The information, provided by the organization, often includes network diagrams, source codes, and IP addressing information of the infrastructure to be tested. Answer A is incorrect. Integration testing

is a logical extension of unit testing. It is performed to identify the problems that occur when two or more units are combined into a component. During integration testing, a developer combines two units that have already been tested into a component, and tests the interface between the two units. Although integration testing can be performed in various ways, the following three approaches are generally used: The top-down approach The bottom-up approach The umbrella approach Answer B is incorrect. Regression testing can be performed any time when a program needs to be modified either to add a feature or to fix an error. It is a process of repeating Unit testing and Integration testing whenever existing tests need to be performed again along with the new tests. Regression testing is performed to ensure that no existing errors reappear, and no new errors are introduced.

NEW QUESTION: 108
Which of the following are the benefits of information classification for an organization? Each correct answer represents a complete solution. Choose two.
A. It helps reduce the Total Cost of Ownership (TCO).
B. It helps identify which protections apply to which information.
C. It helps identify which information is the most sensitive or vital to an organization.
D. It ensures that modifications are not made to data by unauthorized personnel or processes.
Answer: B,C (LEAVE A REPLY)
Following are the benefits of information classification for an organization: It helps identify which protections apply to which information. It helps identify which information is the most sensitive or vital to an organization. It supports the tenets of confidentiality, integrity, and availability as it pertains to data. Answer D is 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 A is incorrect. Information classification cannot reduce the Total Cost of Ownership (TCO).

NEW QUESTION: 109
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
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 110
The NIST Information Security and Privacy Advisory Board (ISPAB) paper "Perspectives on Cloud Computing and Standards" specifies potential advantages and disdvantages of virtualization. Which of the following disadvantages does it include? Each correct answer represents a complete solution. Choose all that apply.
A. It increases capabilities for fault tolerant computing using rollback and snapshot features.
B. It increases intrusion detection through introspection.
C. It initiates the risk that malicious software is targeting the VM environment.
D. It increases overall security risk shared resources.
E. It creates the possibility that remote attestation may not work.
F. It involves new protection mechanisms for preventing VM escape, VM detection, and VM-VM interference.
G. It increases configuration effort because of complexity and composite system.
Answer: C,D,E,F,G (LEAVE A REPLY)
Explanation/Reference:
Explanation: The potential security disadvantages of virtualization are as follows: It increases configuration effort because of complexity and composite system. It initiates the problem of how to prevent overlap while mapping VM storage onto host files. It introduces the problem of virtualizing the TPM. It creates the possibility that remote attestation may not work. It initiates the problem of detecting VM covert channels. It involves new protection mechanisms for preventing

VM escape, VM detection, and VM-VM interference. It initiates the possibility of virtual networking configuration errors. It initiates the risk that malicious software is targeting the VM environment. It increases overall security risk shared resources, such as networks, clipboards, clocks, printers, desktop management, and folders. Answer: A and B are incorrect. These are not the disadvantages of virtualization, as described in the NIST Information Security and Privacy Advisory Board (ISPAB) paper
"Perspectives on Cloud Computing and Standards".

NEW QUESTION: 111
Which of the following processes will you involve to perform the active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures?
A. Penetration testing
B. Baselining
C. Risk analysis
D. Compliance checking
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation: A penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered. It is a component of a full security audit. AnswerC is incorrect. Risk analysis is the science of risks and their probability and evaluation in a business or a process. It is an important factor in security enhancement and prevention in a system. Risk analysis should be performed as part of the risk management process for each project. The outcome of the risk analysis would be the creation or review of the risk register to identify and quantify risk elements to the project and their potential impact. Answer D is incorrect. Compliance checking performs the reviews for safeguards and controls to verify whether the entity is complying with particular procedures, rules or not. It includes the inspection of operational systems to guarantee that hardware and software controls have been correctly implemented and maintained. Compliance checking covers the activities such as penetration testing and vulnerability assessments. Compliance checking must be performed by skilled persons, or by an automated software package. Answer: B is incorrect. Baselining is a method for analyzing the performance of computer networks. The method is marked by comparing the current performance to a historical metric, or

"baseline". For example, if a user measured the performance of a network switch over a period of time, he could use that performance figure as a comparative baseline if he made a configuration change to the switch.

NEW QUESTION: 112
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
E. Explanation:
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: D,E (LEAVE A REPLY)
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.

NEW QUESTION: 113
Which of the following specifies the behaviors of the DRM implementation and any applications that are accessing the implementation?
A. OS fingerprinting
B. OTA provisioning
C. Access control
D. Compliance rule
Answer: D (LEAVE A REPLY)
The Compliance rule specifies the behaviors of the DRM implementation and any applications that are accessing the implementation. The compliance rule specifies the following elements: Definition of specific license rights Device requirements Revocation of license path or penalties when the implementation is not robust enough or noncompliant Answer B is incorrect. 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. Answer C is incorrect. An access control is a system, which enables an authority to control access to areas and resources in a given physical facility, or computer-based information system. Access control system, within

the field of physical security, is generally seen as the second layer in the security of a physical structure. It refers to all mechanisms that control visibility of screens, views, and data within Siebel Business Applications. Answer A is incorrect. OS fingerprinting is a process in which an external host sends special traffic on the external network interface of a computer to determine the computer's operating system. It is one of the primary steps taken by hackers in preparing an attack.

NEW QUESTION: 114
Which of the following terms ensures that no intentional or unintentional unauthorized modification is made to data?
A. Non-repudiation
B. Integrity
C. Authentication
D. Confidentiality
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: Integrity ensures that no intentional or unintentional unauthorized modification is made to data. Answer: D is incorrect. Confidentiality refers to the protection of data against unauthorized access.
Administrators can provide confidentiality by encrypting data. Answer: A is incorrect. Non-repudiation is a mechanism to prove that the sender really sent this message. Answer: C is incorrect. Authentication is the process of verifying the identity of a person or network host.

NEW QUESTION: 115
Which of the following testing methods tests the system efficiency by systematically selecting the suitable and minimum set of tests that are required to effectively cover the affected changes?
A. Unit testing
B. Integration testing
C. Acceptance testing
D. Regression testing
Answer: D (LEAVE A REPLY)
Regression testing focuses on finding defects after a major code change has occurred. Specifically, it seeks to uncover software regressions, or old bugs that have come back. Such regressions occur whenever software functionality that was previously working correctly stops working as intended. Typically, regressions occur as an unintended consequence of program changes, when the newly developed part of the software collides with the previously existing code. Regression testing tests the system efficiency by systematically selecting the suitable and minimum set of tests that are required to effectively cover the affected changes. Answer A is incorrect. Unit testing is a type of testing in which each independent unit of an application is tested separately. During unit testing, a developer takes the smallest unit of an application, isolates it from the rest of the application code, and tests it to determine whether it works as

expected. Unit testing is performed before integrating these independent units into modules. The most common approach to unit testing requires drivers and stubs to be written. Drivers and stubs are programs. A driver simulates a calling unit, and a stub simulates a called unit. Answer C is incorrect. Acceptance testing is performed on the application before its implementation into the production environment. It is done either by a client or an application specialist to ensure that the software meets the requirement for which it was made. Answer B is incorrect. Integration testing is a software testing that seeks to verify the interfaces between components against a software design. Software components may be integrated in an iterative way or all together ("big bang"). Normally the former is considered a better practice since it allows interface issues to be localized more quickly and fixed. Integration testing works to expose defects in the interfaces and interaction between the integrated components (modules). Progressively larger groups of tested software components corresponding to elements of the architectural design are integrated and tested until the software works as a system.

NEW QUESTION: 116
Which of the following actions does the Data Loss Prevention (DLP) technology take when an agent detects a policy violation for data of all states? Each correct answer represents a complete solution.
Choose all that apply.
A. It creates an alert.
B. It quarantines the file to a secure location.
C. It reconstructs the session.
D. It blocks the transmission of content.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: When an agent detects a policy violation for data of all states, the Data Loss prevention (DLP) technology takes one of the following actions: It creates an alert. It notifies an administrator of a violation. It quarantines the file to a secure location. It encrypts the file. It blocks the transmission of content. Answer:
C is incorrect. Data Loss Prevention (DLP) reconstructs the session when data is in motion.

NEW QUESTION: 117
Continuous Monitoring is the fourth phase of the security certification and accreditation process. What activities are performed in the Continuous Monitoring process? Each correct answer represents a complete solution. Choose all that apply.
A. Security accreditation decision
B. Security control monitoring and impact analyses of changes to the information system
C. Security accreditation documentation
D. Configuration management and control
E. Status reporting and documentation
Answer: B,D,E (LEAVE A REPLY)

Explanation/Reference:
Explanation: Continuous Monitoring is the fourth phase of the security certification and accreditation process. The Continuous Monitoring process consists of the following three main activities: Configuration management and control Security control monitoring and impact analyses of changes to the information system Status reporting and documentation The objective of these tasks is to observe and evaluate the information system security controls during the system life cycle. These tasks determine whether the changes that have occurred will negatively impact the system security. Answer: A and C are incorrect.
Security accreditation decision and security accreditation documentation are the two tasks of the security accreditation phase.

NEW QUESTION: 118
What are the differences between managed and unmanaged code technologies? Each correct answer represents a complete solution. Choose two.
A. Managed code is referred to as Hex code, whereas unmanaged code is referred to as byte code.
B. C and C++ are the examples of managed code, whereas Java EE and Microsoft.NET are the examples of unmanaged code.
C. Managed code executes under management of a runtime environment, whereas unmanaged code is executed by the CPU of a computer system.
D. Managed code is compiled into an intermediate code format, whereas unmanaged code is compiled into machine code.
Answer: C,D (LEAVE A REPLY)
Explanation/Reference:
Explanation: Programming languages are categorized into two technologies: 1.Managed code: This computer program code is compiled into an intermediate code format. Managed code is referred to as byte code. It executes under the management of a runtime environment. Java EE and Microsoft.NET are the examples of managed code. 2.Unmanaged code: This computer code is compiled into machine code.
Unmanaged code is executed by the CPU of a computer system. C and C++ are the examples of unmanaged code. AnswerA is incorrect. Managed code is referred to as byte code. Answer B is incorrect. C and C++ are the examples of unmanaged code, whereas Java EE and Microsoft.NET are the examples of managed code.

NEW QUESTION: 119
The mission and business process level is the Tier 2. What are the various Tier 2 activities? Each correct answer represents a complete solution. Choose all that apply.
A. Developing an organization-wide information protection strategy and incorporating high-level information security requirements
B. Defining the types of information that the organization needs, to successfully execute the stated missions and business processes

C. Specifying the degree of autonomy for the subordinate organizations
D. Defining the core missions and business processes for the organization
E. Prioritizing missions and business processes with respect to the goals and objectives of the organization
Answer: (SHOW ANSWER)
The mission and business process level is the Tier 2. It addresses risks from the mission and business process perspective. It is guided by the risk decisions at Tier 1. The various Tier 2 activities are as follows: It defines the core missions and business processes for the organization. It also prioritizes missions and business processes, with respect to the goals and objectives of the organization. It defines the types of information that an organization requires, to successfully execute the stated missions and business processes. It helps in developing an organization-wide information protection strategy and incorporating high-level information security requirements. It specifies the degree of autonomy for the subordinate organizations.

NEW QUESTION: 120
Which of the following is a malicious exploit of a website, whereby unauthorized commands are transmitted from a user trusted by the website?
A. Cross-Site Scripting
B. Injection flaw
C. Side channel attack
D. Cross-Site Request Forgery
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
CSRF (Cross-Site Request Forgery) is a malicious exploit of a website, whereby unauthorized commands are transmitted from a user trusted by the website. It is also known as a one-click attack or session riding.
CSRF occurs when a user is tricked by an attacker into activating a request in order to perform some unauthorized action. It increases data loss and malicious code execution. AnswerA is incorrect. Cross- site scripting (XSS) is a type of computer security vulnerability typically found in web applications which enable malicious attackers to inject client-side script into web pages viewed by other users. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls, such as the same origin policy. Cross-site scripting carried out on websites were roughly 80% of all security vulnerabilities documented by Symantec as of 2007. Their impact may range from a petty nuisance to a significant security risk, depending on the sensitivity of the data handled by the vulnerable site, and the nature of any security mitigations implemented by the site owner. Answer: C is incorrect. A side channel attack is based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms (compare cryptanalysis). For example, timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information which can be exploited to break the system. Many side- channel attacks

require considerable technical knowledge of the internal operation of the system on which the cryptography is implemented. Answer: B is incorrect.
Injection flaws are the vulnerabilities where a foreign agent illegally uses a sub-system. They are the vulnerability holes that can be used to attack a database of Web applications. It is the most common technique of attacking a database. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing involuntary commands or changing data. Injection flaws include XSS (HTML Injection) and SQL Injection.

NEW QUESTION: 121
Which of the following are examples of passive attacks? Each correct answer represents a complete solution. Choose all that apply.
A. Dumpster diving
B. Placing a backdoor
C. Eavesdropping
D. Shoulder surfing
Answer: A,C,D (LEAVE A REPLY)
Explanation/Reference:
Explanation: In eavesdropping, dumpster diving, and shoulder surfing, the attacker violates the confidentiality of a system without affecting its state. Hence, they are considered passive attacks.

NEW QUESTION: 122
Which of the following specifies access privileges to a collection of resources by using the URL mapping?
A. Code Access Security
B. Security constraint
C. Configuration Management
D. Access Management
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: Security constraint is a type of declarative security, which specifies the protection of web content. It also specifies access privileges to a collection of resources by using the URL

mapping. A deployment descriptor is used to define the security constraint. Security constraint includes the following elements: Web resource collection Authorization constraint User data constraint Answer: A is incorrect.
Code Access Security (CAS), in the Microsoft .NET framework, is Microsoft's solution to prevent untrusted code from performing privileged actions. When the CLR (common language runtime) loads an assembly it will obtain evidence for the assembly and use this to identify the code group that the assembly belongs to.
A code group contains a permission set (one or more permissions). Code that performs a privileged action will perform a code access demand, which will cause the CLR to walk up the call stack and examine the permission set granted to the assembly of each method in the call stack. The code groups and permission sets are determined by the administrator of the machine who defines the security policy. Answer: D is incorrect. Access Management is used to grant authorized users the right to use a service, while preventing access to non- authorized users. The Access Management process essentially executes policies defined in IT Security Management. It is sometimes also referred to as Rights Management or Identity Management. It is part of Service Operation and the owner of Access Management is the Access Manager. Access Management is added as a new process to ITIL V3. The sub-processes of Access Management are as follows: Maintain Catalogue of User Roles and Access Profiles Manage User Access Requests Answer: C is incorrect. Configuration Management (CM) is an Information Technology Infrastructure Library (ITIL) IT Service Management (ITSM) process. It tracks all of the individual Configuration Items (CI) in an IT system, which may be as simple as a single server, or as complex as the entire IT department. In large organizations a configuration manager may be appointed to oversee and manage the CM process.

NEW QUESTION: 123
The Systems Development Life Cycle (SDLC) is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems. Which of the following are the different phases of system development life cycle? Each correct answer represents a complete solution. Choose all that apply.
A. Testing
B. Implementation
C. Operation/maintenance
D. Development/acquisition
E. Disposal
F. Initiation
Answer: B,C,D,E,F (LEAVE A REPLY)
The Systems Development Life Cycle (SDLC), or Software Development Life Cycle in systems engineering, information systems, and software engineering, is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems. The concept generally refers to computers or information systems. The following are the five phases

in a generic System Development Life Cycle: 1.Initiation 2.Development/acquisition 3.Implementation 4.Operation/maintenance 5.Disposal

NEW QUESTION: 124
Fill in the blank with the appropriate security mechanism. is a computer hardware mechanism or programming language construct which handles the occurrence of exceptional events.
A. Exception handling
Answer: A (LEAVE A REPLY)
Exception handling is a computer hardware mechanism or programming language construct that handles the occurrence of events. These events occur during the software execution process and interrupt the instruction flow. Exception handling performs the specific activities for managing the exceptional events.

NEW QUESTION: 125
System Authorization is the risk management process. System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. What are the different phases of System Authorization Plan? Each correct answer represents a part of the solution. Choose all that apply.
A. Post-certification
B. Post-Authorization
C. Authorization
D. Pre-certification
E. Certification
Answer: B,C,D,E (LEAVE A REPLY)
Explanation/Reference:
Explanation: The creation of System Authorization Plan (SAP) is mandated by System Authorization.
System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. It consists of four phases: Phase 1 - Pre-certification Phase 2 - Certification Phase 3 - Authorization Phase 4 - Post-Authorization

NEW QUESTION: 126
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
Answer: A (LEAVE A REPLY)

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.

NEW QUESTION: 127
Martha works as a Project Leader for BlueWell Inc. She and her team have developed accounting software. The software was performing well. Recently, the software has been modified. The users of this software are now complaining about the software not working properly. Which of the following actions will she take to test the software?
A. Perform integration testing
B. Perform regression testing
C. Perform unit testing
D. Perform acceptance testing
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: Regression testing can be performed any time when a program needs to be modified either to add a feature or to fix an error. It is a process of repeating Unit testing and Integration testing whenever existing tests need to be performed again along with the new tests. Regression testing is performed to ensure that no existing errors reappear, and no new errors are introduced. AnswerD is incorrect. The acceptance testing is performed on the application before its implementation into the production environment. It is done either by a client or an application specialist to ensure that the software meets the requirement for which it was made. Answer: A is incorrect. Integration testing is a logical extension of unit testing. It is performed to identify the problems that occur when two or more units are combined into a component. During integration testing, a developer combines two units that have already been tested into a component, and tests the interface between the two units. Although integration testing can be performed in various ways, the following three approaches are generally used: The top-down approach The bottom- up approach The umbrella approach Answer: C is incorrect. Unit testing is a type of testing in which each independent unit of an application is tested separately. During unit testing, a developer takes the smallest unit of an application, isolates it from the rest of the application code, and tests it to determine whether it works as expected. Unit testing is performed before integrating these independent units into modules. The most common approach to unit testing requires drivers and stubs to be written. Drivers and stubs are programs. A driver simulates a calling unit, and a stub simulates a called unit.

NEW QUESTION: 128

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

Answer: (SHOW ANSWER)

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.

NEW QUESTION: 129

Which of the following plans is designed to protect critical business processes from natural or man-made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes?

A. Contingency plan

B. Business continuity plan

C. Crisis communication plan

D. Disaster recovery plan

Answer: (SHOW ANSWER)

The business continuity plan is designed to protect critical business processes from natural or man-made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes. 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 C is incorrect. The crisis communication plan can be broadly defined as the plan for the exchange of information before, during, or after a crisis event. It is considered as a sub-specialty of the public relations

profession that is designed to protect and defend an individual, company, or organization facing a public challenge to its reputation. The aim of crisis communication plan is to assist organizations to achieve continuity of critical business processes and information flows under crisis, disaster or event driven circumstances. 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. Answer D is incorrect. A disaster recovery plan should contain data, hardware, and software that can be critical for a business. It should also include the plan for sudden loss such as hard disc crash. The business should use backup and data recovery utilities to limit the loss of data.

NEW QUESTION: 130
Which of the following statements about the authentication concept of information security management is true?
A. It establishes the users' identity and ensures that the users are who they say they are.
B. It ensures the reliable and timely access to resources.
C. It determines the actions and behaviors of a single individual within a system, and identifies that particular individual.
D. It ensures that modifications are not made to data by unauthorized personnel or processes.
Answer: A (LEAVE A REPLY)
The concept of authentication establishes the users' identity and ensures that the users are who they say they are. Answer B is incorrect. The concept of availability ensures the reliable and timely access to data or resources. Answer D is incorrect. The concept of integrity ensures that modifications are not made to data by unauthorized personnel or processes. Answer C is incorrect. The concept of accountability determines the actions and behaviors of a single individual within a system, and identifies that particular individual.

NEW QUESTION: 131
John works as a security manager for SoftTech Inc. He is working with his team on the disaster recovery management plan. One of his team members has a doubt related to the most cost effective DRP testing plan. According to you, which of the following disaster recovery testing plans is the most cost-effective and efficient way to identify areas of overlap in the plan before conducting more demanding training exercises?
A. Full-scale exercise
B. Walk-through drill
C. Structured walk-through test
D. Evacuation drill

Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: The structured walk-through test is also known as the table-top exercise. In structured walk- through test, the team members walkthrough the plan to identify and correct weaknesses and how they will respond to the emergency scenarios by stepping in the course of the plan. It is the most effective and competent way to identify the areas of overlap in the plan before conducting more challenging training exercises. AnswerA is incorrect. In full-scale exercise, the critical systems run at an alternate site.
AnswerB is incorrect. The emergency management group and response teams actually perform their
emergency response functions by walking through the test, without actually initiating recovery procedures.
But it is not much cost effective. AnswerD is incorrect. It is a test performed when personnel walks through the evacuation route to a designated area where procedures for accounting for the personnel are tested.

NEW QUESTION: 132
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
Answer: B (LEAVE A REPLY)
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.

NEW QUESTION: 133
Which of the following statements best describes the difference between the role of a data owner and the role of a data custodian?
A. The custodian makes the initial information classification assignments, and the operations manager implements the scheme.
B. The data owner implements the information classification scheme after the initial assignment by the custodian.
C. The custodian implements the information classification scheme after the initial assignment by the operations manager.
D. The data custodian implements the information classification scheme after the initial assignment by the data owner.
Answer: D (LEAVE A REPLY)
The data owner is responsible for ensuring that the appropriate security controls are in place, for assigning the initial classification to the data to be protected, for approving access requests from other parts of the organization, and for periodically reviewing the data classifications and access rights. Data owners are primarily responsible for determining the data's sensitivity or classification levels, whereas the data custodian has the responsibility for backup, retention, and recovery of data. The data owner delegates these responsibilities to the custodian. Answer B, A, and C are incorrect. These are not the valid answers.

NEW QUESTION: 134
Which of the following statements are true about declarative security? Each correct answer represents a complete solution. Choose all that apply.
A. It is employed in a layer that relies outside of the software code or uses attributes of the code.
B. It applies the security policies on the software applications at their runtime.
C. In this security, authentication decisions are made based on the business logic.
D. In this security, the security decisions are based on explicit statements.
Answer: A,B,D (LEAVE A REPLY)

Explanation/Reference:
Explanation: Declarative security applies the security policies on the software applications at their runtime.
In this type of security, the security decisions are based on explicit statements that confine security behavior. Declarative security applies security permissions that are required for the software application to access the local resources and provides role-based access control to an individual software component and software application. It is employed in a layer that relies outside of the software code or uses attributes of the code. AnswerC is incorrect. In declarative security, authentication decisions are coarse-grained in nature from an operational or external security perspective.

NEW QUESTION: 135
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: (SHOW ANSWER)
Explanation/Reference:
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. AnswerB 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.

NEW QUESTION: 136
Which of the following access control models are used in the commercial sector? Each correct answer represents a complete solution. Choose two.
A. Biba model
B. Clark-Biba model
C. Clark-Wilson model
D. Bell-LaPadula model
Answer: A,C (LEAVE A REPLY)
Explanation/Reference:
Explanation: The Biba and Clark-Wilson access control models are used in the commercial sector. 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. The Clark-Wilson security model provides a foundation for specifying and analyzing an integrity policy for a computing system. Answer: D is incorrect. The Bell-LaPadula access control model is mainly used in military systems. Answer: B is incorrect. There is no such access control model as Clark-Biba.

NEW QUESTION: 137
Which of the following tiers addresses risks from an information system perspective?
A. Tier 0
B. Tier 3
C. Tier 2
D. Tier 1
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: The information system level is the tier 3. It addresses risks from an information system perspective, and is guided by the risk decisions at tiers 1 and 2. Risk decisions at tiers 1 and 2 impact the ultimate selection and deployment of requisite safeguards. This also has an impact on the countermeasures at the information system level. The RMF primarily operates at tier3 but it can also have interactions at tiers 1 and 2. AnswerA is incorrect. It is an invalid Tier description. Answer: D is incorrect.
The Organization Level is the Tier 1, and it addresses risks from an organizational perspective. AnswerC is incorrect. The mission and business process level is the Tier 2, and it addresses risks from the mission and business process perspective.

NEW QUESTION: 138
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)

Answer: A (LEAVE A REPLY)
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).

NEW QUESTION: 139
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
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: Assessment, monitoring, and assurance determines the necessary compliance that are offered by risk management practices and assessment of risk levels.

NEW QUESTION: 140
An authentication method uses smart cards as well as usernames and passwords for authentication.
Which of the following authentication methods is being referred to?
A. Anonymous
B. Mutual
C. Multi-factor
D. Biometrics
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: Multi-factor authentication involves a combination of multiple methods of authentication. For example, an authentication method that uses smart cards as well as usernames and passwords can be referred to as multi-factor authentication. AnswerB is incorrect. Mutual authentication is a process in which a client process and server are required to prove their identities to each other before performing any application function. The client and server identities can be verified through a trusted third party and use shared secrets as in the case of Kerberos v5.

The MS-CHAP v2 and EAP-TLS authentication methods support mutual authentication. Answer A is incorrect. Anonymous authentication is an authentication method used for Internet communication. It provides limited access to specific public folders and directory information. It is supported by all clients and is used to access unsecured content in public folders. An administrator must create a user account in IIS to enable the user to connect anonymously. Answer: D is incorrect. Biometrics authentication uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user.

NEW QUESTION: 141
Which of the following attacks causes software to fail and prevents the intended users from accessing software?
A. Enabling attack
B. Reconnaissance attack
C. Sabotage attack
D. Disclosure attack
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: A sabotage attack is an attack that causes software to fail. It also prevents the intended users from accessing software. A sabotage attack is referred to as a denial of service (DoS) or compromise of availability. Answer: B is incorrect. The reconnaissance attack enables an attacker to collect information about software and operating environment. Answer: D is incorrect. The disclosure attack exposes the revealed data to an attacker. Answer: A is incorrect. The enabling attack delivers an easy path for other attacks.

NEW QUESTION: 142
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.
Answer: B,C,D (LEAVE A REPLY)
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.

NEW QUESTION: 143
An authentication method uses smart cards as well as usernames and passwords for authentication. Which of the following authentication methods is being referred to?
A. Anonymous

B. Mutual
C. Multi-factor
D. Biometrics
Answer: (SHOW ANSWER)
Multi-factor authentication involves a combination of multiple methods of authentication. For example, an authentication method that uses smart cards as well as usernames and passwords can be referred to as multi-factor authentication. Answer B is incorrect. Mutual authentication is a process in which a client process and server are required to prove their identities to each other before performing any application function. The client and server identities can be verified through a trusted third party and use shared secrets as in the case of Kerberos v5. The MS-CHAP v2 and EAP-TLS authentication methods support mutual authentication. Answer A is incorrect. Anonymous authentication is an authentication method used for Internet communication. It provides limited access to specific public folders and directory information. It is supported by all clients and is used to access unsecured content in public folders. An administrator must create a user account in IIS to enable the user to connect anonymously. Answer D is incorrect. Biometrics authentication uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user.

NEW QUESTION: 144
Which of the following are the principle duties performed by the BIOS during POST (power-on-self-test)?
Each correct answer represents a part of the solution. Choose all that apply.
A. It provides a user interface for system's configuration.
B. It identifies, organizes, and selects boot devices.
C. It delegates control to other BIOS, if it is required.
D. It discovers size and verifies system memory.
E. It verifies the integrity of the BIOS code itself.
F. It interrupts the execution of all running programs.
Answer: A,B,C,D,E (LEAVE A REPLY)
Explanation/Reference:
Explanation: The principle duties performed by the BIOS during POST (power-on-self-test) are as follows:
It verifies the integrity of the BIOS code itself. It discovers size and verifies system memory. It discovers, initializes, and catalogs all system hardware. It delegates control to other BIOS if it is required. It provides a user interface for system's configuration. It identifies, organizes, and selects boot devices. It executes the bootstrap program. AnswerF is incorrect. The BIOS does not interrupt the execution of all running programs.

NEW QUESTION: 145

Which of the following security controls will you use for the deployment phase of the SDLC to build secure software? Each correct answer represents a complete solution. Choose all that apply.

A. Change and Configuration Control

B. Security Certification and Accreditation (C&A)

C. Vulnerability Assessment and Penetration Testing

D. Risk Adjustments

Answer: B,C,D (LEAVE A REPLY)

The various security controls in the SDLC deployment phase are as follows: Secure Installation: While performing any software installation, it should kept in mind that the security configuration of the environment should never be reduced. If it is reduced then security issues and overall risks can affect the environment. Vulnerability Assessment and Penetration Testing: Vulnerability assessments (VA) and penetration testing (PT) is used to determine the risk and attest to the strength of the software after it has been deployed. Security Certification and Accreditation (C&A): Security certification is the process used to ensure controls which are effectively implemented through established verification techniques and procedures, giving organization officials confidence that the appropriate safeguards and countermeasures are in place as means of protection. Accreditation is the provisioning of the necessary security authorization by a senior organization official to process, store, or transmit information. Risk Adjustments: Contingency plans and exceptions should be generated so that the residual risk be above the acceptable threshold.

NEW QUESTION: 146

Which of the following organizations assists the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies?

A. OMB

B. NIST

C. NSA/CSS

D. DCAA

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Explanation: The Office of Management and Budget (OMB) is a Cabinet-level office, and is the largest office within the Executive Office of the President (EOP) of the United States. The current OMB Director is Peter Orszag and was appointed by President Barack Obama. The OMB's predominant mission is to assist the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies. In helping to formulate the President's spending plans, the OMB evaluates the effectiveness of agency programs, policies, and procedures, assesses competing funding demands among agencies, and sets funding priorities. The OMB ensures that agency reports, rules, testimony, and proposed legislation are consistent with the President's Budget and with Administration policies.

Answer D is incorrect. The DCAA has the aim to monitor contractor costs and perform contractor audits.
Answer C is incorrect. The National Security Agency/Central Security Service (NSA/CSS) is a crypto-logic
intelligence agency of the United States government. It is administered as part of the United States Department of Defense. NSA is responsible for the collection and analysis of foreign communications and foreign signals intelligence, which involves cryptanalysis. NSA is also responsible for protecting U.S.
government communications and information systems from similar agencies elsewhere, which involves cryptography. NSA is a key component of the U.S. Intelligence Community, which is headed by the Director of National Intelligence. The Central Security Service is a co-located agency created to coordinate intelligence activities and co-operation between NSA and U.S. military cryptanalysis agencies. NSA's work is limited to communications intelligence. It does not perform field or human intelligence activities. Answer:
B is incorrect. The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory which is a non- regulatory agency of the United States Department of Commerce. The institute's official mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.

NEW QUESTION: 147
Which of the following software review processes increases the software security by removing the common vulnerabilities, such as format string exploits, race conditions, memory leaks, and buffer overflows?
A. Management review
B. Code review
C. Peer review
D. Software audit review
Answer: B (LEAVE A REPLY)
A code review is a systematic examination of computer source code, which searches and resolves issues occurred in the initial development phase. It increases the software security by removing common vulnerabilities, such as format string exploits, race conditions, memory leaks, and buffer overflows. A code review is performed in the following forms: Pair programming Informal walkthrough Formal inspection Answer C is incorrect. A peer review is an examination process in which author and one or more colleagues examine a work product, such as document, code, etc., and evaluate technical content and quality. According to the Capability Maturity Model, peer review offers a systematic engineering practice in order to detect and resolve issues occurring in the software artifacts, and stops the leakage into field operations. Answer A is incorrect. Management review is a management study into a project's status and allocation of resources. Answer D is incorrect. In software audit review one or more auditors, who are not

members of the software development organization, perform an independent examination of a software product, software process, or a set of software processes for assessing compliance with specifications, standards, contractual agreements, or other specifications.

NEW QUESTION: 148
You have a storage media with some data and you make efforts to remove this data. After performing this, you analyze that the data remains present on the media. Which of the following refers to the above mentioned condition?
A. Object reuse
B. Degaussing
C. Residual
D. Data remanence
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation: Data remanence refers to the data that remains even after the efforts have been made for removing or erasing the data. This event occurs because of data being left intact by an insignificant file deletion operation, by storage media reformatting, or through physical properties of the storage medium.
Data remanence can make unintentional disclosure of sensitive information possible. So, it is required that the storage media is released into an uncontrolled environment. Answer: C and B are incorrect. These are the made-up disasters. Answer: A is incorrect. Object reuse refers to reassigning some other object of a storage media that has one or more objects.

NEW QUESTION: 149
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
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: 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. AnswerB 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). AnswerC is incorrect. There is no such access control model as Policy Access Control.

NEW QUESTION: 150
You work as a security manager for BlueWell Inc. You are going through the NIST SP 800-37 C&A methodology, which is based on four well defined phases. In which of the following phases of NIST SP
800-37 C&A methodology does the security categorization occur?
A. Security Accreditation
B. Security Certification
C. Continuous Monitoring
D. Initiation
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation: The various phases of NIST SP 800-37 C&A 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.

NEW QUESTION: 151
Security controls are safeguards or countermeasures to avoid, counteract, or minimize security risks. Which of the following are types of security controls? Each correct answer represents a complete solution. Choose all that apply.
A. Common controls
B. Hybrid controls
C. Storage controls
D. System-specific controls
E. Explanation:
Security controls are safeguards or countermeasures to avoid, counteract, or
minimize security risks. The following are the types of security controls for information systems, that can be employed by an organization: 1.System-specific controls: These types of security controls provide security capability for a particular information system only. 2.Common controls: These types of security controls provide security capability for multiple information systems.

3.Hybrid controls: These types of security controls have features of both system-specific and common controls.

Answer: A,B,D,E (LEAVE A REPLY)

is incorrect. It is an invalid control.

NEW QUESTION: 152

In which of the following deployment models of cloud is the cloud infrastructure operated exclusively for an organization?

A. Public cloud

B. Community cloud

C. Private cloud

D. Hybrid cloud

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation: In private cloud, the cloud infrastructure is operated exclusively for an organization. The private cloud infrastructure is administered by the organization or a third party, and exists on premise and off premise.

NEW QUESTION: 153

In which of the following IDS evasion attacks does an attacker send a data packet such that IDS accepts the data packet but the host computer rejects it?

A. Evasion attack

B. Fragmentation overlap attack

C. Fragmentation overwrite attack

D. Insertion attack

Answer: (SHOW ANSWER)

In an insertion attack, an IDS accepts a packet and assumes that the host computer will also accept it. But in reality, when a host system rejects the packet, the IDS accepts the attacking string that will exploit vulnerabilities in the IDS. Such attacks can badly infect IDS signatures and IDS signature analysis. Answer B is incorrect. In this approach, an attacker sends packets in such a manner that one packet fragment overlaps data from a previous fragment. The information is organized in the packets in such a manner that when the victim's computer reassembles the

packets, an attack string is executed on the victim's computer. Since the attacking string is in fragmented form, IDS is unable to detect it. Answer C is incorrect. In this approach, an attacker sends packets in such a manner that one packet fragment overwrites data from a previous fragment. The information is organized into the packets in such a manner that when the victim's computer reassembles the packets, an attack string is executed on the victim's computer. Since the attacking string is in fragmented form, IDS becomes unable to detect it. Answer A is incorrect. An evasion attack is one in which an IDS rejects a malicious packet but the host computer accepts it. Since an IDS has rejected it, it does not check the contents of the packet. Hence, using this technique, an attacker can exploit the host computer. In many cases, it is quite simple for an attacker to send such data packets that can easily perform evasion attacks on an IDSs.

NEW QUESTION: 154
Which of the following is a standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system?
A. FITSAF
B. FIPS
C. TCSEC
D. SSAA
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: Trusted Computer System Evaluation Criteria (TCSEC) is a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. TCSEC was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information. It was replaced with the development of the Common Criteria international standard originally published in 2005. The TCSEC, frequently referred to as the Orange Book, is the centerpiece of the DoD Rainbow Series publications. AnswerD 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. Answer: A is incorrect. FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. It provides an approach for federal agencies. It determines how federal agencies are meeting existing policy and establish goals. The main advantage of FITSAF is that it addresses the requirements of Office of Management and Budget (OMB). It also addresses the guidelines provided by the National Institute of Standards and Technology (NIsT). Answer: B is incorrect. The Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States federal government for use by all non-

military government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community (ANSI, IEEE, ISO, etc.). Some FIPS standards were originally developed by the U.S. government. For instance, standards for encoding data (e.g., country codes), but more significantly some encryption standards, such as the Data Encryption Standard (FIPS 46-
3) and the Advanced Encryption Standard (FIPS 197). In 1994, NOAA (Noaa) began broadcasting coded signals called FIPS (Federal Information Processing System) codes along with their standard weather broadcasts from local stations. These codes identify the type of emergency and the specific geographic area (such as a county) affected by the emergency.

NEW QUESTION: 155
Which of the following processes culminates in an agreement between key players that a system in its current configuration and operation provides adequate protection controls?
A. Information Assurance (IA)
B. Information systems security engineering (ISSE)
C. Certification and accreditation (C&A)
D. Risk Management
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: Certification and accreditation (C&A) is a set of processes that culminate in an agreement between key players that a system in its current configuration and operation provides adequate protection controls. Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The C&A process is used extensively in the U.S. Federal Government. Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed- upon set of security controls. Answer: D is incorrect. Risk management is a set of processes that ensures a risk-based approach is used to determine adequate, cost- effective security for a system. Answer: A is incorrect. Information assurance (IA) is the process of organizing and monitoring information-related risks.
It ensures that only the approved users have access to the approved information at the approved time. IA practitioners seek to protect and defend information and information systems by ensuring confidentiality, integrity, authentication, availability, and non-repudiation. These objectives are applicable whether the information is in storage, processing, or transit, and whether threatened by

an attack. Answer: B is incorrect. ISSE is a set of processes and solutions used during all phases of a system's life cycle to meet the system's information protection needs.

NEW QUESTION: 156
Which of the following statements describe the main purposes of a Regulatory policy? Each correct answer represents a complete solution. Choose all that apply.
A. It acknowledges the importance of the computing resources to the business model
B. It provides a statement of support for information security throughout the enterprise
C. It ensures that an organization is following the standard procedures or base practices of operation in its specific industry.
D. It gives an organization the confidence that it is following the standard and accepted industry policy.
Answer: C,D (LEAVE A REPLY)
Explanation/Reference:
Explanation: The main purposes of a Regulatory policy are as follows: It ensures that an organization is following the standard procedures or base practices of operation in its specific industry. It gives an organization the confidence that it is following the standard and accepted industry policy. AnswerB and A are incorrect. These are the policy elements of Senior Management Statement of Policy.

NEW QUESTION: 157
The service-oriented modeling framework (SOMF) introduces five major life cycle modeling activities that drive a service evolution during design-time and run-time. Which of the following activities integrates SOA software assets and establishes SOA logical environment dependencies?
A. Service-oriented discovery and analysis modeling
B. Service-oriented business integration modeling
C. Service-oriented logical architecture modeling
D. Service-oriented logical design modeling
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: The service-oriented logical architecture modeling integrates SOA software assets and establishes SOA logical environment dependencies. It also offers foster service reuse, loose coupling and consolidation. AnswerA is incorrect. The service-oriented discovery and analysis modeling discovers and analyzes services for granularity, reusability, interoperability, loose-coupling, and identifies consolidation opportunities. Answer B is incorrect. The service-oriented business integration modeling identifies service integration and alignment opportunities with business domains' processes. Answer: D is incorrect. The service-oriented logical design modeling establishes service relationships and message exchange paths.

NEW QUESTION: 158

Which of the following elements sets up a requirement to receive the constrained requests over a protected layer connection, such as TLS (Transport Layer Security)?

A. User data constraint

B. Authorization constraint

C. Web resource collection

D. Accounting constraint

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation: User data constraint is a security constraint element summarized in the Java Servlet Specification 2.4. It sets up a requirement to receive the constrained requests over a protected layer connection, such as TLS (Transport Layer Security). The user data constraint offers guarantee (NONE, INTEGRAL, and CONFEDENTIAL) for the transportation of data between client and server. If a request does not have user data constraint, the container accepts the request after it is received on a connection.

AnswerC is incorrect. Web resource collection is a set of URL patterns and HTTP operations that define

all resources required to be protected. It is a security constraint element summarized in the Java Servlet Specification v2.4. The Web resource collection includes the following elements: URL patterns HTTP methods AnswerB is incorrect. Authorization constraint is a security constraint element summarized in the Java Servlet Specification 2.4. It sets up a requirement for authentication and names the authorization roles that can access the URL patterns and HTTP methods as defined by the security constraint. In the absence of a security constraint, the container accepts the request without requiring any user authentication. If no authorization role is specified in the authorization constraint, the container cannot access constrained requests. The wildcard character "*" specifies all authorization role names that are defined in the deployment descriptor. AnswerD is incorrect. It is not a security constraint element.

NEW QUESTION: 159

Numerous information security standards promote good security practices and define frameworks or systems to structure the analysis and design for managing information security controls. Which of the following are the U.S. Federal Government information security standards? Each correct answer represents a complete solution. Choose all that apply.

A. IR Incident Response

B. Information systems acquisition, development, and maintenance

C. SA System and Services Acquisition

D. CA Certification, Accreditation, and Security Assessments

Answer: A,C,D (LEAVE A REPLY)

Following are the various U.S. Federal Government information security standards: AC Access Control AT Awareness and Training AU Audit and Accountability CA Certification, Accreditation, and Security Assessments CM Configuration Management CP Contingency Planning IA Identification and Authentication IR Incident Response MA Maintenance MP Media Protection PE

Physical and Environmental Protection PL Planning PS Personnel Security RA Risk Assessment SA System and Services Acquisition SC System and Communications Protection SI System and Information Integrity Answer B is incorrect. Information systems acquisition, development, and maintenance is an International information security standard.

NEW QUESTION: 160
SIMULATION
Fill in the blank with an appropriate phrase. models address specifications, requirements, design, verification and validation, and maintenance activities.
Answer:
Life cycle
Explanation/Reference:
Explanation: A life cycle model helps to provide an insight into the development process and emphasizes on the relationships among the different activities in this process. This model describes a structured approach to the development and adjustment process involved in producing and maintaining systems. The life cycle model addresses specifications, design, requirements, verification and validation, and maintenance activities.

NEW QUESTION: 161
You work as a Security Manager for Tech Perfect Inc. The company has a Windows based network. It is required to determine compatibility of the systems with custom applications. Which of the following techniques will you use to accomplish the task?
A. Safe software storage
B. Antivirus management
C. Backup control
D. Software testing
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation: In order to accomplish the task, you should use the software testing technique. By using this technique you can determine compatibility of systems with custom applications or you can identify other unforeseen interactions. You can also use the software testing technique while you are upgrading software. AnswerB is incorrect. You can use the antivirus management to save the systems from viruses, unexpected software interactions, and the subversion of security controls. Answer: A is incorrect. You can use the safe software storage technique to ensure that the software and backup copies have not been modified without authorization. Answer: C is incorrect. You can use the backup control to perform back up of software and data.

NEW QUESTION: 162
Which of the following characteristics are described by the DIAP Information Readiness Assessment function? Each correct answer represents a complete solution. Choose all that apply.
A. It provides for entry and storage of individual system data.

B. It performs vulnerability/threat analysis assessment.
C. It provides data needed to accurately assess IA readiness.
D. It identifies and generates IA requirements.
Answer: B,C,D (LEAVE A REPLY)
The characteristics of the DIAP Information Readiness Assessment function are as follows: It provides data needed to accurately assess IA readiness. It identifies and generates IA requirements. It performs vulnerability/threat analysis assessment. Answer A is incorrect. It is a function performed by the ASSET system.

NEW QUESTION: 163
Which of the following classification levels defines the information that, if disclosed to the unauthorized parties, could be reasonably expected to cause exceptionally grave damage to the national security?
A. Secret information
B. Unclassified information
C. Confidential information
D. Top Secret information
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: Top Secret information is the highest level of classification of material on a national level.
Such material would cause "exceptionally grave damage" to national security if publicly available.
Answer:
A is incorrect. Secret information is that, if disclosed to unauthorized parties, could be expected to cause serious damage to the national security, but it is not the best answer for the above question. AnswerC is incorrect. Such material would cause "damage" or be "prejudicial" to national security if publicly available.
AnswerB is incorrect. Unclassified information, technically, is not a classification level, but is used for
government documents that do not have a classification listed above. Such documents can sometimes be viewed by those without security clearance.

NEW QUESTION: 164
You work as a system engineer for BlueWell Inc. You want to verify that the build meets its data requirements, and correctly generates each expected display and report. Which of the following tests will help you to perform the above task?
A. Performance test
B. Functional test
C. Reliability test
D. Regression test
Answer: B (LEAVE A REPLY)

Explanation/Reference:
Explanation: 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.

NEW QUESTION: 165
Which of the following NIST Special Publication documents provides a guideline on network security testing?
A. NIST SP 800-42
B. NIST SP 800-53A
C. NIST SP 800-60
D. NIST SP 800-53
E. NIST SP 800-37
F. NIST SP 800-59
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: NIST SP 800-42 provides a guideline on network security testing. Answer: E, D, B, F, and C are incorrect. 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.

NEW QUESTION: 166
In which of the following IDS evasion attacks does an attacker send a data packet such that IDS accepts the data packet but the host computer rejects it?
A. Evasion attack
B. Fragmentation overlap attack
C. Fragmentation overwrite attack
D. Insertion attack

Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation: In an insertion attack, an IDS accepts a packet and assumes that the host computer will also accept it. But in reality, when a host system rejects the packet, the IDS accepts the attacking string that will exploit vulnerabilities in the IDS. Such attacks can badly infect IDS signatures and IDS signature analysis.
AnswerB is incorrect. In this approach, an attacker sends packets in such a manner that one packet
fragment overlaps data from a previous fragment. The information is organized in the packets in such a manner that when the victim's computer reassembles the packets, an attack string is executed on the victim's computer. Since the attacking string is in fragmented form, IDS is unable to detect it. AnswerC is incorrect. In this approach, an attacker sends packets in such a manner that one packet fragment overwrites data from a previous fragment. The information is organized into the packets in such a manner that when the victim's computer reassembles the packets, an attack string is executed on the victim's computer. Since the attacking string is in fragmented form, IDS becomes unable to detect it. Answer A is incorrect. An evasion attack is one in which an IDS rejects a malicious packet but the host computer accepts it. Since an IDS has rejected it, it does not check the contents of the packet. Hence, using this technique, an attacker can exploit the host computer. In many cases, it is quite simple for an attacker to send such data packets that can easily perform evasion attacks on an IDSs.

NEW QUESTION: 167
Which of the following configuration management system processes keeps track of the changes so that the latest acceptable configuration specifications are readily available?
A. Configuration Control
B. Configuration Status and Accounting
C. Configuration Verification and Audit
D. Configuration Identification
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: 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. The configuration status and accounting process keeps track of the changes so that the latest acceptable configuration specifications are readily available.
AnswerC is incorrect. The verification and audit processes seek to establish a high level of confidence in
how well the Configuration Management activity is working. AnswerA 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.
AnswerD 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.

NEW QUESTION: 168
Which of the following methods can be helpful to eliminate social engineering threat? Each correct answer represents a complete solution. Choose three.
A. Password policies
B. Data classification
C. Data encryption
D. Vulnerability assessments
Answer: A,B,D (LEAVE A REPLY)
The following methods can be helpful to eliminate social engineering threat: Password policies Vulnerability assessments Data classification Password policy should specify that how the password can be shared. Company should implement periodic penetration and vulnerability assessments. These assessments usually consist of using known hacker tools and common hacker techniques to breach a network security. Social engineering should also be used for an accurate assessment. Since social engineers use the knowledge of others to attain information, it is essential to have a data classification model in place that all employees know and follow. Data classification assigns level of sensitivity of company information. Each classification level specifies that who can view and edit data, and how it can be shared.

NEW QUESTION: 169
Which of the following approaches can be used to build a security program? Each correct answer represents a complete solution. Choose all that apply.
A. Right-Up Approach
B. Left-Up Approach

C. Top-Down Approach
D. Bottom-Up Approach
Answer: C,D (LEAVE A REPLY)
Explanation/Reference:
Explanation: Top-Down Approach is an approach to build a security program. The initiation, support, and direction come from the top management and work their way through middle management and then to staff members. It is treated as the best approach. This approach ensures that the senior management, who is ultimately responsible for protecting the company assets, is driving the program. Bottom-Up Approach is an approach to build a security program. The lower-end team comes up with a security control or a program without proper management support and direction. It is less effective and doomed to fail. Answer:
A and B are incorrect. No such types of approaches exist

NEW QUESTION: 170
Which of the following plans is documented and organized for emergency response, backup operations, and recovery maintained by an activity as part of its security program that will ensure the availability of critical resources and facilitates the continuity of operations in an emergency situation?
A. Continuity Of Operations Plan
B. Business Continuity Plan
C. Contingency Plan
D. Disaster Recovery Plan
Answer: C (LEAVE A REPLY)
Contingency plan is prepared and documented for emergency response, backup operations, and recovery maintained by an activity as the element of its security program that will ensure the availability of critical resources and facilitates the continuity of operations in an emergency situation. 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. Answer D is incorrect. A disaster recovery plan should contain data, hardware, and software that can be critical for a business. It should also include the plan for sudden loss such as hard disc crash. The business should use backup and data recovery utilities to limit the loss of data. Answer A 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 B 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.

NEW QUESTION: 171
Which of the following technologies is used by hardware manufacturers, publishers, copyright holders and individuals to impose limitations on the usage of digital content and devices?
A. Hypervisor
B. Grid computing
C. Code signing
D. Digital rights management
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: Digital rights management (DRM) is an access control technology used by hardware manufacturers, publishers, copyright holders and individuals to impose limitations on the usage of digital content and devices. It describes the technology that prevents the uses of digital content that were not desired or foreseen by the content provider. DRM does not refer to other forms of copy protection which can be circumvented without modifying the file or device, such as serial numbers or keyfiles. It can also refer to restrictions associated with specific instances of digital works or devices. Answer C is incorrect.
Code signing is the process of digitally signing executables and scripts in order to confirm the software author, and guarantee that the code has not been altered or corrupted since it is signed by use of a cryptographic hash. Answer A is incorrect. A hypervisor is a virtualization technique that allows multiple operating systems (guests) to run concurrently on a host computer. It is also called the virtual machine monitor (VMM). The hypervisor provides a virtual operating platform to the guest operating systems and checks their execution process. It provides isolation to the host's resources. The hypervisor is installed on server hardware. Answer: B is incorrect. Grid computing refers to the combination of computer resources from multiple administrative domains to achieve a common goal.

NEW QUESTION: 172
Security is a state of well-being of information and infrastructures in which the possibilities of successful yet undetected theft, tampering, and/or disruption of information and services are kept low or tolerable. Which of the following are the elements of security? Each correct answer represents a complete solution. Choose all that apply.
A. Integrity
B. Authenticity
C. Confidentiality
D. Availability
Answer: (SHOW ANSWER)

Explanation/Reference:
Explanation: The elements of security are as follows: 1.Confidentiality: It is the concealment of information or resources. 2.Authenticity: It is the identification and assurance of the origin of information. 3.Integrity: It refers to the trustworthiness of data or resources in terms of preventing improper and unauthorized changes. 4.Availability: It refers to the ability to use the information or resources as desired.

NEW QUESTION: 173
Mark is the project manager of the NHQ project in StarTech Inc. The project has an asset valued at $195,000 and is subjected to an exposure factor of 35 percent. What will be the Single Loss Expectancy of the project?
A. $68,250
B. $92,600
C. $72,650
D. $67,250
Answer: A (LEAVE A REPLY)
The Single Loss Expectancy (SLE) of this project will be $68,250. Single Loss Expectancy is a term related to Risk Management and Risk Assessment. It can be defined as the monetary value expected from the occurrence of a risk on an asset. It is mathematically expressed as follows: Single Loss Expectancy (SLE) = Asset Value (AV) * Exposure Factor (EF) where the Exposure Factor is represented in the impact of the risk over the asset, or percentage of asset lost. As an example, if the Asset Value is reduced two thirds, the exposure factor value is .66. If the asset is completely lost, the Exposure Factor is 1.0. The result is a monetary value in the same unit as the Single Loss Expectancy is expressed. Here, it is as follows: SLE = Asset Value * Exposure Factor = 195,000 * 0.35 = $68,250 Answer B, C, and D are incorrect. These are not valid SLE's for this project.

NEW QUESTION: 174
SIMULATION
Fill in the blank with an appropriate phrase. A is defined as any activity that has an effect on defining, designing, building, or executing a task, requirement, or procedure.
Answer:
technical effort
Explanation/Reference:
Explanation: A technical effort is described as any activity, which has an effect on defining, designing, building, or implementing a task, requirement, or procedure. The technical effort is an element of technical management that is required to progress efficiently and effectively from a business need to the deployment and operation of the system.

NEW QUESTION: 175

Which of the following statements reflect the 'Code of Ethics Canons' in the '(ISC)2 Code of Ethics'? Each correct answer represents a complete solution. Choose all that apply.

A. Act honorably, honestly, justly, responsibly, and legally.

B. Give guidance for resolving good versus good and bad versus bad dilemmas.

C. Provide diligent and competent service to principals.

D. Protect society, the commonwealth, and the infrastructure.

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation: The Code of Ethics Canons in (ISC)2 code of ethics are as follows: Protect society, the commonwealth, and the infrastructure. Act honorably, honestly, justly, responsibly, and legally. Provide diligent and competent service to principals. Advance and protect the profession.

NEW QUESTION: 176

To help review or design security controls, they can be classified by several criteria . One of these criteria is based on their nature. According to this criterion, which of the following controls consists of incident response processes, management oversight, security awareness, and training?

A. Compliance control

B. Physical control

C. Procedural control

D. Technical control

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation: Procedural controls include incident response processes, management oversight, security awareness, and training. Answer: B is incorrect. Physical controls include fences, doors, locks, and fire extinguishers. Answer: D is incorrect. Technical controls include user authentication (login) and logical access controls, antivirus software, and firewalls. Answer: A is incorrect. The legal and regulatory, or compliance controls, include privacy laws, policies, and clauses.

NEW QUESTION: 177

Which of the following processes describes the elements such as quantity, quality, coverage, timelines, and availability, and categorizes the different functions that the system will need to perform in order to gather the documented mission/business needs?

A. Human factors

B. Functional requirements

C. Performance requirements

D. Operational scenarios

E. Explanation:

The functional requirements categorize the different functions that the system will need to perform in order to gather the documented mission/business needs. The functional requirements describe the elements such as quantity, quality, coverage, timelines, and availability.

Answer: B (LEAVE A REPLY)
is incorrect. The performance requirements comprise of speed, throughput, accuracy, humidity tolerances, mechanical stresses such as vibrations or noises. Answer A is incorrect. Human factor consists of factors, which affect the operation of the system or component, such as design space, eye movement, or ergonomics. Answer D is incorrect. The operational scenarios provide assistance to the system designers and form the basis of major events in the acquisition phases, such as testing the products for system integration. The customer classifies and defines the operational scenarios, which indicate the range of anticipated uses of system products.

NEW QUESTION: 178
Which of the following cryptographic system services ensures that information will not be disclosed to any unauthorized person on a local network?
A. Authentication
B. Integrity
C. Non-repudiation
D. Confidentiality
Answer: (SHOW ANSWER)
The confidentiality service of a cryptographic system ensures that information will not be disclosed to any unauthorized person on a local network.

NEW QUESTION: 179
Which of the following are Service Level Agreement (SLA) structures as defined by ITIL? Each correct answer represents a complete solution. Choose all that apply.
A. Component Based
B. Service Based
C. Segment Based
D. Customer Based
E. Multi-Level
Answer: B,D,E (LEAVE A REPLY)
Explanation/Reference:
Explanation: ITIL defines 3 types of Service Level Agreement (SLA) structures, which are as follows:
1.Customer Based: It covers all services used by an individual customer group. 2.Service Based: It is one service for all customers. 3.Multi-Level: Some examples of Multi-Level SLA are 3 Tier SLA encompassing Corporate and Customer & Service Layers. AnswerC and A are incorrect. There are no such SLA structures as Segment Based and Component Based.

NEW QUESTION: 180
Which of the following tools is used to attack the Digital Watermarking?
A. Steg-Only Attack
B. Active Attacks

C. 2Mosaic
D. Gifshuffle
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: 2Mosaic is a tool used for watermark breaking. It is an attack against a digital watermarking system. In this type of attack, an image is chopped into small pieces and then placed together. When this image is embedded into a web page, the web browser renders the small pieces into one image. This image looks like a real image with no watermark in it. This attack is successful, as it is impossible to read watermark in very small pieces. Answer: D is incorrect. Gifshuffle is used to hide message or information inside GIF images. It is done by shuffling the colormap. This tool also provides compression and encryption. Answer: B and A are incorrect. Active Attacks and Steg-Only Attacks are used to attack Steganography.

NEW QUESTION: 181
The rights of an author or a corporation to make profit from the creation of their products (such as software, music, etc.) are protected by the Intellectual Property law. Which of the following are the components of the Intellectual Property law? Each correct answer represents a part of the solution. Choose two.
A. Trademark law
B. Industrial Property law
C. Copyright law
D. Patent law
Answer: B,C (LEAVE A REPLY)
The Industrial Property law and the Copyright law are the components of the Intellectual Property law.

NEW QUESTION: 182
Which of the following process areas does the SSE-CMM define in the 'Project and Organizational Practices' category? Each correct answer represents a complete solution. Choose all that apply.
A. Provide Ongoing Skills and Knowledge
B. Verify and Validate Security

C. Manage Project Risk
D. Improve Organization's System Engineering Process
Answer: (SHOW ANSWER)
Project and Organizational Practices include the following process areas: PA12: Ensure Quality PA13: Manage Configuration PA14: Manage Project Risk PA15: Monitor and Control Technical Effort PA16: Plan Technical Effort PA17: Define Organization's System Engineering Process PA18: Improve Organization's System Engineering Process PA19: Manage Product Line Evolution PA20: Manage Systems Engineering Support Environment PA21: Provide Ongoing Skills and Knowledge PA22: Coordinate with Suppliers

NEW QUESTION: 183
John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we-are- secure.com. You have searched all open ports of the we-are-secure server. Now, you want to perform the next information-gathering step, i.e., passive OS fingerprinting. Which of the following tools can you use to accomplish the task?
A. Superscan
B. NBTscan
C. Nmap
D. P0f
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation: According to the scenario, you have searched all open ports of the we-are-secure server.
Now you want to perform the next information-gathering step, i.e., passive OS fingerprinting. For this, you will use the P0f tool to accomplish the task. P0f is a passive OS fingerprinting tool that is used to identify the operating system of a target host simply by examining captured packets even when the device is behind a packet firewall. It does not generate any additional direct or indirect network traffic. P0f can also be used to gather various information, such as firewall presence, NAT use (for policy enforcement), existence of a load balancer setup, the distance to the remote system and its uptime, etc. AnswerC is incorrect. Nmap is used for active OS fingerprinting. Nmap is a free open-source utility for network exploration and security auditing. It is used to discover computers and services on a computer network, thus creating a "map" of the network. Just like many simple port scanners, Nmap is capable of discovering passive services. In addition, Nmap may be able to determine various details about the remote computers.
These include operating system, device type, uptime, software product used to run a service, exact version number of that product, presence of some firewall techniques and, on a local area network, even vendor of the remote network card. Nmap runs on Linux, Microsoft Windows etc.AnswerA is incorrect. SuperScan is a TCP/UDP port scanner. It also works as a ping sweeper and hostname resolver. It can ping a given range of IP addresses and resolve the host name of the remote system.The features of SuperScan are as follows: It scans any port range from a built-in list or any given range. It performs ping scans and port scans using any IP range. It modifies

the port list and port descriptions using the built in editor. It connects to any discovered open port using user-specified "helper" applications. It has the transmission speed control utility.
AnswerB is incorrect. NBTscan is a scanner that scans IP networks for NetBIOS name information. It
sends a NetBIOS status query to each address in a supplied range and lists received information in human readable form. It displays IP address, NetBIOS computer name, logged-in user name and MAC address of each responded host. NBTscan works in the same manner as nbtstat, but it operates on a range of addresses instead of just one.

NEW QUESTION: 184
Which of the following is NOT a responsibility of a data owner?
A. Approving access requests
B. Ensuring that the necessary security controls are in place
C. Delegating responsibility of the day-to-day maintenance of the data protection mechanisms to the data custodian
D. Maintaining and protecting data
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: It is not a responsibility of a data owner. The data custodian (information custodian) is responsible for maintaining and protecting the data.
AnswerB, A, and C are incorrect. All of these are responsibilities of a data owner. The roles and responsibilities of a data owner are as follows: The data owner (information owner) is usually a member of management, in charge of a specific business unit, and is ultimately responsible for the protection and use of a specific subset of information. The data owner decides upon the classification of the data that he is responsible for and alters that classification if the business needs arise. This person is also responsible for ensuring that the necessary security controls are in place, ensuring that proper access rights are being used, defining security requirements per classification and backup requirements, approving any disclosure activities, and defining user access criteria. The data owner approves access requests or may choose to delegate this function to business unit managers. And it is the data owner who will deal with security violations pertaining to the data he is responsible for protecting. The data owner, who obviously has enough on his plate, delegates responsibility of the day-to-day maintenance of the data protection mechanisms to the data custodian.

NEW QUESTION: 185
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: (SHOW ANSWER)
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.

NEW QUESTION: 186
What are the security advantages of virtualization, as described in the NIST Information Security and Privacy Advisory Board (ISPAB) paper "Perspectives on Cloud Computing and Standards"? Each correct answer represents a complete solution. Choose three.
A. It increases capabilities for fault tolerant computing.
B. It adds a layer of security for defense-in-depth.
C. It decreases exposure of weak software.
D. It decreases configuration effort.
Answer: A,B,C (LEAVE A REPLY)
The security advantages of virtualization are as follows: It adds a layer of security for defense-in-depth. It provides strong encapsulation of errors. It increases intrusion detection through introspection. It decreases exposure of weak software. It increases the flexibility for discovery. It increases capabilities for fault tolerant computing using rollback and snapshot features. Answer D is incorrect. Virtualization increases configuration effort because of complexity of the virtualization layer and composite system.

NEW QUESTION: 187
Which of the following is an attack with IP fragments that cannot be reassembled?
A. Password guessing attack
B. Teardrop attack
C. Dictionary attack
D. Smurf attack
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: Teardrop is an attack with IP fragments that cannot be reassembled. In this attack, corrupt packets are sent to the victim's computer by using IP's packet fragmentation algorithm. As a result of this attack, the victim's computer might hang. AnswerD is incorrect. Smurf is an ICMP attack that involves spoofing and flooding. AnswerC is incorrect. Dictionary attack is a type of password guessing attack. This type of attack uses a dictionary of common words to find out the password of a user. It can also use common words in either upper or lower case to find a password. There are many programs available on the Internet to automate and execute dictionary

attacks. AnswerA is incorrect. A password guessing attack occurs when an unauthorized user tries to log on repeatedly to a computer or network by guessing usernames and passwords. Many password guessing programs that attempt to break passwords are available on the Internet. Following are the types of password guessing attacks: Brute force attack Dictionary attack

NEW QUESTION: 188
Which of the following can be used to accomplish authentication? Each correct answer represents a complete solution. Choose all that apply.
A. Encryption
B. Biometrics
C. Token
D. Password
Answer: B,C,D (LEAVE A REPLY)
Explanation/Reference:
Explanation: The following can be used to accomplish authentication: 1.Password 2.Biometrics 3.Token A password is a secret word or string of characters that is used for authentication, to prove identity, or gain access to a resource.

NEW QUESTION: 189
You are advising a school district on disaster recovery plans. In case a disaster affects the main IT centers for the district they will need to be able to work from an alternate location. However, budget is an issue. Which of the following is most appropriate for this client?
A. Cold site
B. Off site
C. Warm site
D. Hot site
Answer: (SHOW ANSWER)
A cold site provides an office space, and in some cases basic equipment. However, you will need to restore your data to that equipment in order to use it. This is a much less expensive solution than the hot site. Answer D is incorrect. A hot site has equipment installed, configured and ready to use. This may make disaster recovery much faster, but will also be more expensive. And a school district can afford to be down for several hours before resuming IT operations, so the less expensive option is more appropriate. Answer C is incorrect. A warm site is between a hot and cold site. It has some equipment ready and connectivity ready. However, it is still significantly more expensive than a cold site, and not necessary for this scenario. Answer B is incorrect. Off site is not any type of backup site terminology.

NEW QUESTION: 190
You work as a CSO (Chief Security Officer) for Tech Perfect Inc. You have a disaster scenario and you want to discuss it with your team members for getting appropriate responses of the disaster. In which of the following disaster recovery tests can this task be performed?

A. Structured walk-through test
B. Full-interruption test
C. Parallel test
D. Simulation test
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation: A simulation test is a method used to test the disaster recovery plans. It operates just like a structured walk-through test. In the simulation test, the members of a disaster recovery team present with a disaster scenario and then, discuss on appropriate responses. These suggested responses are measured and some of them are taken by the team. The range of the simulation test should be defined carefully for avoiding excessive disruption of normal business activities. AnswerA is incorrect. The structured walk- through test is also known as the table-top exercise. In structured walk-through test, the team members walkthrough the plan to identify and correct weaknesses and how they will respond to the emergency scenarios by stepping in the course of the plan. It is the most effective and competent way to identify the areas of overlap in the plan before conducting more challenging training exercises. Answer: B is incorrect.
A full-interruption test includes the operations that shut down at the primary site and are shifted to the recovery site according to the disaster recovery plan. It operates just like a parallel test. The full- interruption test is very expensive and difficult to arrange. Sometimes, it causes a major disruption of operations if the test fails. AnswerC is incorrect. A parallel test includes the next level in the testing procedure, and relocates the employees to an alternate recovery site and implements site activation procedures. These employees present with their disaster recovery responsibilities as they would for an actual disaster. The disaster recovery sites have full responsibilities to conduct the day-to-day organization's business.

NEW QUESTION: 191
In which of the following deployment models of cloud is the cloud infrastructure operated exclusively for an organization?
A. Public cloud
B. Community cloud
C. Private cloud
D. Hybrid cloud
Answer: (SHOW ANSWER)
In private cloud, the cloud infrastructure is operated exclusively for an organization.
The private cloud infrastructure is administered by the organization or a third party, and exists on premise and off premise.

NEW QUESTION: 192
Which of the following scanning techniques helps to ensure that the standard software configuration is currently with the latest security patches and software, and helps to locate uncontrolled or unauthorized software?

A. Port Scanning
B. Discovery Scanning
C. Server Scanning
D. Workstation Scanning
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation: Workstation scanning provides help to ensure that the standard software configuration exists with the most recent security patches and software. It helps to locate uncontrolled or unauthorized software. A full workstation vulnerability scan of the standard corporate desktop configuration must be implemented on a regularly basis. AnswerB is incorrect. The discovery scanning technique is used to gather adequate information regarding each network device to identify what type of device it is, its operating system, and if it is running any externally vulnerable services, like Web services, FTP, or email.
AnswerC is incorrect. A full server vulnerability scan helps to determine if the server OS has been configured to the corporate standards and identify if applications have been updated with the latest security patches and software versions. AnswerA is incorrect. Port scanning technique describes the process of sending a data packet to a port to gather information about the state of the port.

NEW QUESTION: 193
Which of the following components of configuration management involves periodic checks to determine the consistency and completeness of accounting information and to verify that all configuration management policies are being followed?
A. Configuration Identification
B. Configuration Auditing
C. Configuration Control
D. Configuration Status Accounting
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: Configuration auditing is a component of configuration management, which involves periodic checks to establish the consistency and completeness of accounting information and to confirm 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. AnswerD 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. AnswerC 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.
AnswerA 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.

NEW QUESTION: 194
The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise. What are the responsibilities of a Chief Information Officer?
Each correct answer represents a complete solution. Choose all that apply.
A. Facilitating the sharing of security risk-related information among authorizing officials
B. Preserving high-level communications and working group relationships in an organization
C. Establishing effective continuous monitoring program for the organization
D. Proposing the information technology needed by an enterprise to achieve its goals and then working within a budget to implement the plan
Answer: B,C,D (LEAVE A REPLY)
Explanation/Reference:
Explanation: A Chief Information Officer (CIO) plays the role of a leader. The responsibilities of a Chief Information Officer are as follows: Establishes effective continuous monitoring program for the organization. Facilitates continuous monitoring process for the organizations. Preserves high-level communications and working group relationships in an organization.
Confirms that information systems are covered by a permitted security plan and monitored throughout the System Development Life Cycle (SDLC). Manages and delegates decisions to employees in large enterprises. Proposes the information technology needed by an enterprise to achieve its goals and then works within a budget to implement the plan. AnswerA is incorrect. A Risk Executive facilitates the sharing of security risk-related information among authorizing officials.

NEW QUESTION: 195
You are the project manager of QSL project for your organization. You are working with your project team and several key stakeholders to create a diagram that shows how various elements

of a system interrelate and the mechanism of causation within the system. What diagramming technique are you using as a part of the risk identification process?

A. Cause and effect diagrams

B. Influence diagrams

C. Predecessor and successor diagramming

D. System or process flowcharts

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation: In this example you are using a system or process flowchart. These can help identify risks within the process flow, such as bottlenecks or redundancy. Answer: A is incorrect. A cause and effect diagram, also known as an Ishikawa or fishbone diagram, can reveal causal factors to the effect to be solved. Answer: B is incorrect. An influence diagram shows causal influences, time ordering of events and relationships among variables and outcomes. Answer: C is incorrect. Predecessor and successor diagramming is not a valid risk identification term.

NEW QUESTION: 196

Which of the following test methods has the objective to test the IT system from the viewpoint of a threat- source and to identify potential failures in the IT system protection schemes?

A. Security Test and Evaluation (ST&E)

B. Penetration testing

C. Automated vulnerability scanning tool

D. On-site interviews

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Explanation: The goal of penetration testing is to examine the IT system from the perspective of a threat- source, and to identify potential failures in the IT system protection schemes. Penetration testing, when performed in the risk assessment process, is used to assess an IT system's capability to survive with the intended attempts to thwart system security. AnswerA is incorrect. The objective of ST&E is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards.

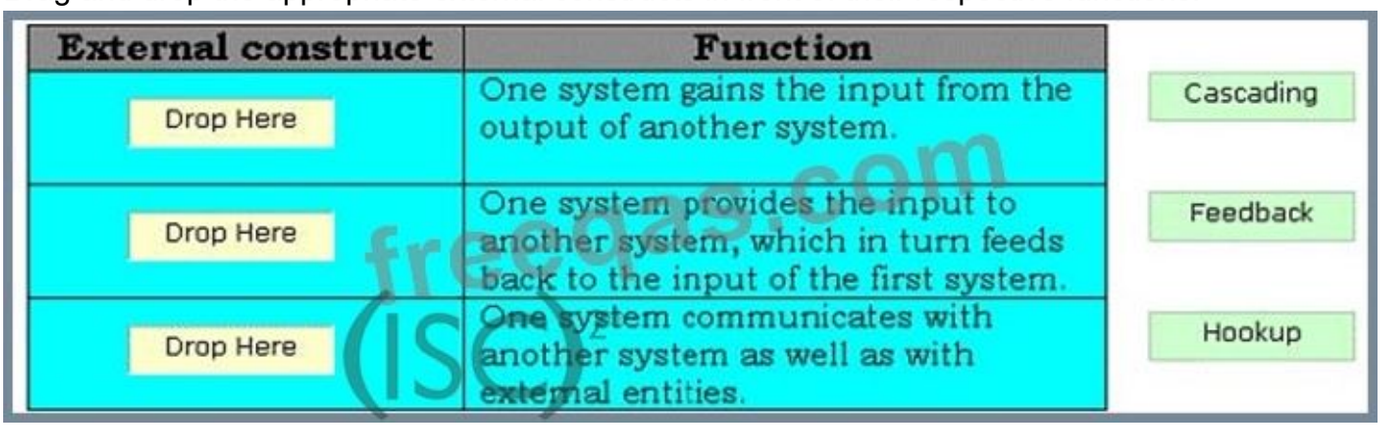
NEW QUESTION: 197
Henry is the project manager of the QBG Project for his company. This project has a budget of $4,576,900 and is expected to last 18 months to complete. The CIO, a stakeholder in the project, has introduced a scope change request for additional deliverables as part of the project work. What component of the change control system would review the proposed changes' impact on the features and functions of the project's product?
A. Configuration management system
B. Scope change control system
C. Cost change control system
D. Integrated change control
Answer: A (LEAVE A REPLY)
The configuration management system ensures that proposed changes to the project's scope are reviewed and evaluated for their affect on the project's product. Configuration Management System is a subsystem of the overall project management system. It is a collection of formal documented procedures used to identify and document the functional and physical characteristics of a product, result, service, or component of the project. It also controls any changes to such characteristics, and records and reports each change and its implementation status. It includes the documentation, tracking systems, and defined approval levels necessary for authorizing and controlling changes. Audits are performed as part of configuration management to determine if the requirements have been met. Answer B is incorrect. The scope change control system focuses on reviewing the actual changes to the project scope. When a change to the project's scope is proposed, the configuration management system is also invoked. Answer C is incorrect. The cost change control system is responsible for reviewing and controlling changes to the project costs. Answer D is incorrect. Integrated change control examines the affect of a proposed change on the project as a whole.

NEW QUESTION: 198
Penetration testing (also called pen testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit. Which of the following areas can be exploited in a penetration test? Each correct answer represents a complete solution. Choose all that apply.
A. Kernel flaws
B. Information system architectures
C. Race conditions
D. File and directory permissions
E. Buffer overflows
F. Trojan horses
G. Social engineering
Answer: A,C,D,E,F,G (LEAVE A REPLY)
Penetration testing (also called pen testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit. Following are the areas

that can be exploited in a penetration test: Kernel flaws: Kernel flaws refer to the exploitation of kernel code flaws in the operating system. Buffer overflows: Buffer overflows refer to the exploitation of a software failure to properly check for the length of input data. This overflow can cause malicious behavior on the system. Race conditions: A race condition is a situation in which an attacker can gain access to a system as a privileged user. File and directory permissions: In this area, an attacker exploits weak permissions restrictions to gain unauthorized access of documents. Trojan horses: These are malicious programs that can exploit an information system by attaching themselves in valid programs and files. Social engineering: In this technique, an attacker uses his social skills and persuasion to acquire valuable information that can be used to conduct an attack against a system.

NEW QUESTION: 199
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.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: 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. AnswerA is incorrect. It is not one of the primary functions of configuration management. It is the function of risk avoidance.

NEW QUESTION: 200
DRAG DROP
Drag and drop the appropriate external constructs in front of their respective functions.



Answer:

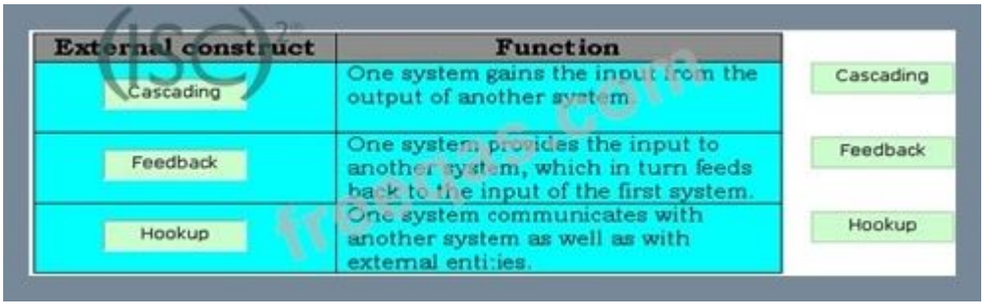
External construct	Function
Cascading	One system gains the input from the output of another system.
Feedback	One system provides the input to another system, which in turn feeds back to the input of the first system.
Hookup	One system communicates with another system as well as with external entities.

Cascading

Feedback

Hookup

Explanation:



There are two types of compositional constructs: 1.External constructs: The various types of external constructs are as follows: Cascading: In this type of external construct, one system gains the input from the output of another system. Feedback: In this type of external construct, one system provides the input to another system, which in turn feeds back to the input of the first system. Hookup: In this type of external construct, one system communicates with another system as well as with external entities. 2.Internal constructs: The internal constructs include intersection, union, and difference.

NEW QUESTION: 201

In which of the following architecture styles does a device receive input from connectors and generate transformed outputs?

A. N-tiered

B. Heterogeneous

C. Pipes and filters

D. Layered

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation: In the pipes and filters architecture style, a device receives input from connectors and generates transformed outputs. A pipeline has a series of processing elements in which the output of each element works as an input of the next element. A little amount of buffering is provided between the two successive elements.

NEW QUESTION: 202

Which of the following is a standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system?

A. FITSAF

B. FIPS
C. TCSEC
D. SSAA
Answer: (SHOW ANSWER)
Trusted Computer System Evaluation Criteria (TCSEC) is a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. TCSEC was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information. It was replaced with the development of the Common Criteria international standard originally published in 2005. The TCSEC, frequently referred to as the Orange Book, is the centerpiece of the DoD Rainbow Series publications. Answer D 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. Answer A is incorrect. FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. It provides an approach for federal agencies. It determines how federal agencies are meeting existing policy and establish goals. The main advantage of FITSAF is that it addresses the requirements of Office of Management and Budget (OMB). It also addresses the guidelines provided by the National Institute of Standards and Technology (NIsT). Answer B is incorrect. The Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States federal government for use by all non-military government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community (ANSI, IEEE, ISO, etc.). Some FIPS standards were originally developed by the U.S. government. For instance, standards for encoding data (e.g., country codes), but more significantly some encryption standards, such as the Data Encryption Standard (FIPS 46-3) and the Advanced Encryption Standard (FIPS 197). In 1994, NOAA (Noaa) began broadcasting coded signals called FIPS (Federal Information Processing System) codes along with their standard weather broadcasts from local stations. These codes identify the type of emergency and the specific geographic area (such as a county) affected by the emergency.

NEW QUESTION: 203
You work as an analyst for Tech Perfect Inc. You want to prevent information flow that may cause a conflict of interest in your organization representing competing clients. Which of the following security models will you use?
A. Bell-LaPadula model
B. Chinese Wall model

C. Clark-Wilson model
D. Biba model
Answer: (SHOW ANSWER)
The Chinese Wall Model is the basic security model developed by Brewer and Nash. This model prevents information flow that may cause a conflict of interest in an organization representing competing clients. The Chinese Wall Model provides both privacy and integrity for data. Answer D 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. Answer C 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 A 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.

NEW QUESTION: 204
Which of the following are the common roles with regard to data in an information classification program?
Each correct answer represents a complete solution. Choose all that apply.
A. Editor
B. Custodian
C. Owner
D. User
E. Security auditor
Answer: B,C,D,E (LEAVE A REPLY)
Explanation/Reference:
Explanation: The following are the common roles with regard to data in an information classification program: Owner Custodian User Security auditor The following are the responsibilities of the owner with regard to data in an information classification program: Determining what level of classification the information requires. Reviewing the classification assignments at regular time intervals and making changes as the business needs change. Delegating the responsibility of the data protection duties to the custodian. The following are the

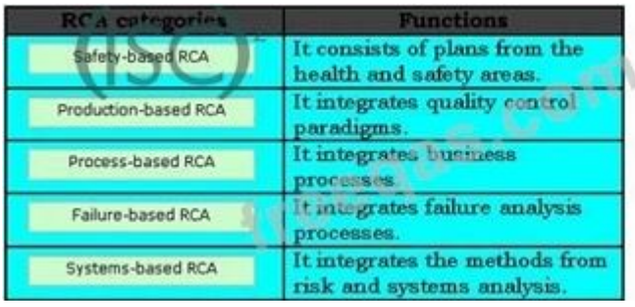
responsibilities of the custodian with regard to data in an information classification program: Running regular backups and routinely testing the validity of the backup data Performing data restoration from the backups when necessary Controlling access, adding and removing privileges for individual users The users must comply with the requirements laid out in policies and procedures. They must also exercise due care. A security auditor examines an organization's security procedures and mechanisms.

NEW QUESTION: 205
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.
Answer: B,C,D (LEAVE A REPLY)
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.

NEW QUESTION: 206
Fill in the blank with an appropriate phrase. is used to provide security mechanisms for the storage, processing, and transfer of data.
A. Data classification
Answer: A (LEAVE A REPLY)
Data classification is used to protect the data based on its sensitivity, secrecy, and confidentiality. It provides security mechanisms for storage, processing, and transfer of data. Data classification also helps to verify the effort, funds, and resources allocated to save the data, and controls access to it.

NEW QUESTION: 207
DRAG DROP
RCA (root cause analysis) is an iterative and reactive method that identifies the root cause of various incidents, and the actions required to prevent these incidents from reoccurring. RCA is classified in various categories. Choose appropriate categories and drop them in front of their respective functions.
Select and Place:

Answer:



Explanation/Reference:

The various categories of root cause analysis (RCA) are as follows: Safety-based RC A.
It consists of plans from the health and safety areas. Production-based RCA. It integrates quality control paradigms. Process-based RCA. It integrates business processes. Failure-based RCA. It integrates failure analysis processes as employed in engineering and maintenance. Systems-based RCA. It integrates the methods from risk and systems analysis.

NEW QUESTION: 208

Which of the following NIST documents provides a guideline for identifying an information system as a National Security System?

A. NIST SP 800-37
B. NIST SP 800-59
C. NIST SP 800-53
D. NIST SP 800-60
E. NIST SP 800-53A

Answer: B (LEAVE A REPLY)

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.

NEW QUESTION: 209
ISO 27003 is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Which of the following elements does this standard contain? Each correct answer represents a complete solution. Choose all that apply.
A. Inter-Organization Co-operation
B. Information Security Risk Treatment
C. CSFs (Critical success factors)
D. ystem requirements for certification bodies Managements
E. Terms and Definitions
F. Guidance on process approach
Answer: A,C,E,F (LEAVE A REPLY)
Explanation/Reference:
Explanation: ISO 27003 is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is entitled as "Information Technology - Security techniques - Information security management system implementation guidance".
The ISO 27003 standard provides guidelines for implementing an ISMS (Information Security Management System). It mainly focuses upon the PDCA method along with establishing, implementing, reviewing, and improving the ISMS itself. The ISO 27003 standard contains the following elements: Introduction Scope Terms and Definitions CSFs (Critical success factors) Guidance on process approach Guidance on using PDCA Guidance on Plan Processes Guidance on Do Processes Guidance on Check Processes Guidance on Act Processes Inter-Organization Co-operation AnswerB is incorrect. This element is included in the ISO 27005 standard. AnswerD is incorrect. This element is included in the ISO 27006 standard.

NEW QUESTION: 210
John works as a security manager for SoftTech Inc. He is working with his team on the disaster recovery management plan. One of his team members has a doubt related to the most cost effective DRP testing plan. According to you, which of the following disaster recovery testing plans is the most cost-effective and efficient way to identify areas of overlap in the plan before conducting more demanding training exercises?
A. Full-scale exercise
B. Walk-through drill
C. Structured walk-through test
D. Evacuation drill
Answer: C (LEAVE A REPLY)
The structured walk-through test is also known as the table-top exercise. In structured walk-through test, the team members walkthrough the plan to identify and correct weaknesses and how they will respond to the emergency scenarios by stepping in the course of the plan. It is the most effective and competent way to identify the areas of overlap in the plan before conducting

more challenging training exercises. Answer A is incorrect. In full-scale exercise, the critical systems run at an alternate site. Answer B is incorrect. The emergency management group and response teams actually perform their emergency response functions by walking through the test, without actually initiating recovery procedures. But it is not much cost effective. Answer D is incorrect. It is a test performed when personnel walks through the evacuation route to a designated area where procedures for accounting for the personnel are tested.

NEW QUESTION: 211
Which of the following processes provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and the security posture of a system or site?
A. NSA-IAM
B. NIACAP
C. ASSET
D. DITSCAP
Answer: B (LEAVE A REPLY)
NIACAP is a process, which provides a standard set of activities, general tasks, and a management structure to certify and accredit systems that maintain the information assurance and the security posture of a system or site. Answer D is incorrect. DITSCAP is a process, which establishes a standard process, a set of activities, general task descriptions, and a management structure to certify and accredit the IT systems that will maintain the required security posture. Answer A is incorrect. The NSA-IAM evaluates information systems at a high level and uses a subset of the SSE-CMM process areas to measure the implementation of information security on these systems. Answer C is incorrect. ASSET is a tool developed by NIST to automate the process of self-assessment through the use of the questionnaire in NIST.

NEW QUESTION: 212
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 (LEAVE A REPLY)

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.

NEW QUESTION: 213

Which of the following attacks causes software to fail and prevents the intended users from accessing software?

A. Enabling attack

B. Reconnaissance attack

C. Sabotage attack

D. Disclosure attack

Answer: C (LEAVE A REPLY)

A sabotage attack is an attack that causes software to fail. It also prevents the intended users from accessing software. A sabotage attack is referred to as a denial of service (DoS) or compromise of availability. Answer B is incorrect. The reconnaissance attack enables an attacker to collect information about software and operating environment. Answer D is incorrect. The disclosure attack exposes the revealed data to an attacker. Answer A is incorrect. The enabling attack delivers an easy path for other attacks.