ISC.CSSLP.v2022-08-12.q154

Exam Code:	CSSLP
Exam Name:	Certified Secure Software Lifecycle Professional Practice Test
Certification Provider:	ISC
Free Question Number:	154
Version:	v2022-08-12
# of views:	2352
# of Questions views:	1540
https://www.dumpsdb.com/dumps/ISC/CSSLP/ISC.CSSLP.v2022-08-12.q154	

NEW QUESTION: 1
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)
Explanation/Reference:
Explanation: 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
AnswerB, C, and D are incorrect. These are not valid SLE's for this project.

NEW QUESTION: 2
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)
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: 3
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)
Physical Configuration Audit (PCA) is one of the practices used in Software Configuration Management for Software Configuration Auditing. The purpose of the software PCA is to ensure that the design and reference documentation is consistent with the as-built software product. PCA checks and matches the really implemented layout with the documented layout. Answer C is incorrect. Functional Configuration Audit or FCA is one of the practices used in Software Configuration Management for Software Configuration Auditing. FCA occurs either at delivery or at the moment of effecting the change. A Functional Configuration Audit ensures that functional and performance attributes of a configuration item are achieved. Answer B is incorrect. Configuration control is a procedure of the Configuration management. Configuration control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them. It supports the change of the functional and physical attributes of software at various points in time, and performs systematic control of changes to the identified attributes. Answer A is incorrect. Configuration identification is the process of identifying the attributes that

define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined. Baselining an attribute forces formal configuration change control processes to be effected in the event that these attributes are changed.

NEW QUESTION: 4
Which of the following are the tasks performed by the owner in the information classification schemes? Each correct answer represents a part of the solution. Choose three.
A. To make original determination to decide what level of classification the information requires, which is based on the business requirements for the safety of the data.
B. To review the classification assignments from time to time and make alterations as the business requirements alter.
C. To perform data restoration from the backups whenever required.
D. To delegate the responsibility of the data safeguard duties to the custodian.
Answer: (SHOW ANSWER)
The different tasks performed by the owner are as follows: He makes the original determination to decide what level of classification the information requires, which is based on the business requirements for the safety of the data. He reviews the classification assignments from time to time and makes alterations as the business needs change. He delegates the responsibility of the data safeguard duties to the custodian. He specifies controls to ensure confidentiality, integrity and availability. Answer C is incorrect. This task is performed by the custodian and not by the owner.

NEW QUESTION: 5
Who amongst the following makes the final accreditation decision?
A. ISSE
B. CRO
C. DAA
D. ISSO
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: The DAA, also known as Authorizing Official, makes the final accreditation decision. 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. 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. AnswerA is incorrect. 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. AnswerB 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.

NEW QUESTION: 6
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: 7
Which of the following terms refers to a mechanism which proves that the sender really sent a particular message?
A. Confidentiality
B. Non-repudiation
C. Authentication
D. Integrity

Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: Non-repudiation is a mechanism which proves that the sender really sent a message. It provides an evidence of the identity of the senderand message integrity. It also prevents a person from denying the submission or delivery of the message and the integrity of its contents. AnswerC is incorrect.
Authentication is a process of verifying the identity of a person or network host. AnswerA is incorrect.
Confidentiality ensures that no one can read a message except the intended receiver. AnswerD is incorrect. Integrity assures the receiver that the received message has not been altered in any way from the original.

NEW QUESTION: 8
You work as a Security Manager for Tech Perfect Inc. You want to save all the data from the SQL injection attack, which can read sensitive data from the database and modify database data using some commands, such as Insert, Update, and Delete. Which of the following tasks will you perform? Each correct answer represents a complete solution. Choose three.
A. Apply maximum number of database permissions.
B. Use an encapsulated library for accessing databases.
C. Create parameterized stored procedures.
D. Create parameterized queries by using bound and typed parameters.
Answer: B,C,D (LEAVE A REPLY)
Explanation/Reference:
Explanation: The methods of mitigating SQL injection attacks are as follows: 1.Create parameterized queries by using bound and typed parameters. 2.Create parameterized stored procedures. 3.Use a encapsulated library in order to access databases. 4.Minimize database permissions. AnswerA is incorrect. In order to save all the data from the SQL injection attack, you should minimize database permissions.

NEW QUESTION: 9
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: 10
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: 11
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: 12
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: (SHOW ANSWER)
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: 13

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 3, Validation

B. Phase 1, Definition

C. Phase 2, Verification

D. Phase 4, Post Accreditation Phase

Answer: (SHOW ANSWER)

Phase 4, Post Accreditation Phase of the DITSCAP includes the activities, which 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. Answer B 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 C 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 A is incorrect. Phase 3 validates the compliance of a fully integrated system with the information stated in the SSAA.

NEW QUESTION: 14

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: A,B,D (LEAVE A REPLY)

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: 15

You work as a systems engineer for BlueWell Inc. Which of the following tools will you use to look outside your own organization to examine how others achieve their performance levels, and what processes they use to reach those levels?

A. Benchmarking

B. Six Sigma

C. ISO 9001:2000

D. SEI-CMM

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Explanation: Benchmarking is the tool used by system assessment process to provide a point of reference by which performance measurements can be reviewed with respect to other organizations. Benchmarking is also recognized as Best Practice Benchmarking or Process Benchmarking. It is a process used in management and mostly useful for strategic management. It is the process of comparing the business processes and performance metrics including cost, cycle time, productivity, or quality to another that is widely considered to be an industry standard benchmark or best practice. It allows organizations to develop plans on how to implement best practice with the aim of increasing some aspect of performance.

Benchmarking might be a one-time event, although it is frequently treated as a continual process in which organizations continually seek out to challenge their practices. It allows organizations to develop plans on how to make improvements or adapt specific best practices, usually with the aim of increasing some aspect of performance. Answer: C is incorrect. The ISO 9001:2000 standard combines the three standards

9001, 9002, and 9003 into one, called 9001. Design and development procedures are required only if a company does in fact engage in the creation of new products. The 2000 version sought to make a radical change in thinking by actually placing the concept of process management front and center ("Process management" was the monitoring and optimizing of a company's tasks and activities, instead of just inspecting the final product). The ISO 9001:2000 version also demands involvement by upper executives, in order to integrate quality into the business system and avoid delegation of quality functions to junior administrators. Another goal is to improve effectiveness via process performance metrics numerical measurement of the effectiveness of tasks and activities. Expectations of continual process improvement and tracking customer satisfaction were made explicit. Answer: B is incorrect. Six Sigma is a business management strategy, initially implemented by Motorola. As of 2009 it enjoys widespread application in many sectors of industry, although its application is not without controversy. Six Sigma seeks to improve the quality of process outputs by identifying and removing the causes of defects and variability in manufacturing and business processes. It uses a set of quality management methods, including statistical methods, and creates a special infrastructure of people within the organization ("Black Belts", "Green Belts", etc.) who are experts in these methods. Each Six Sigma project carried out within an organization follows a defined sequence of steps and has quantified financial targets (cost reduction or profit increase).

The often used Six Sigma symbol is as follows:

Answer D is incorrect. Capability Maturity Model Integration (CMMI) was created by Software Engineering
Institute (SEI). CMMI in software engineering and organizational development is a process improvement approach that provides organizations with the essential elements for effective process improvement. It can be used to guide process improvement across a project, a division, or an entire organization. CMMI can help integrate traditionally separate organizational functions, set process improvement goals and priorities, provide guidance for quality processes, and provide a point of reference for appraising current processes.
CMMI is now the de facto standard for measuring the maturity of any process. Organizations can be assessed against the CMMI model using Standard CMMI Appraisal Method for Process Improvement (SCAMPI).

NEW QUESTION: 16
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: (SHOW ANSWER)
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: 17

Which of the following DITSCAP C&A phases takes place between the signing of the initial version of the SSAA and the formal accreditation of the system?

A. Phase 4

B. Phase 3

C. Phase 1

D. Phase 2

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation: 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. Answer: C, B, and A are incorrect. These phases do not take place between the signing of the initial version of the SSAA and the formal accreditation of the system.

NEW QUESTION: 18

DRAG DROP

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

Select and Place:

Answer:

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

Explanation/Reference:

Explanation: The various DoD policy series are as follows:

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

NEW QUESTION: 19

Which of the following NIST Special Publication documents provides a guideline on questionnaires and checklists through which systems can be evaluated for compliance against specific control objectives?

A. NIST SP 800-37

B. NIST SP 800-26

C. NIST SP 800-53A

D. NIST SP 800-59

E. NIST SP 800-53

F. NIST SP 800-60

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Explanation: NIST SP 800-26 (Security Self-Assessment Guide for Information Technology Systems) provides a guideline on questionnaires and checklists through which systems can be evaluated for compliance against specific control objectives. AnswerA, E, C, D, and F 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: 20
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)
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. Answer C is incorrect. This option comes under vulnerability scanning.

NEW QUESTION: 21
Which of the following DoD policies establishes policies and assigns responsibilities to achieve DoD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network-centric warfare?
A. DoDI 5200.40
B. DoD 8500.1 Information Assurance (IA)
C. DoD 8510.1-M DITSCAP
D. DoD 8500.2 Information Assurance Implementation
Answer: B (LEAVE A REPLY)
DoD 8500.1 Information Assurance (IA) sets up policies and allots responsibilities to achieve DoD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network-centric warfare. DoD 8500.1 also summarizes the roles and responsibilities for the persons responsible for carrying out the IA policies. Answer D is incorrect. The DoD 8500.2 Information Assurance Implementation pursues 8500.1. It provides assistance on how to implement policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks. DoD Instruction 8500.2 allots tasks and sets procedures for applying integrated layered protection of the DOD information systems and networks in accordance with the DoD 8500.1 policy. It also provides some important guidelines on how to implement an IA program. Answer A is incorrect. DoDI 5200.40 executes the policy, assigns responsibilities, and recommends procedures under reference for Certification and Accreditation(C&A) of information technology (IT). Answer C is incorrect. DoD 8510.1-M DITSCAP provides standardized activities leading to accreditation, and establishes a process and management baseline.

NEW QUESTION: 22
Which of the following is generally used in packages in order to determine the package or product tampering?
A. Tamper resistance
B. Tamper evident
C. Tamper data
D. Tamper proof
Answer: (SHOW ANSWER)
Tamper resistance is resistance tampered by the users of a product, package, or system, or the users who can physically access it. It includes simple as well as complex devices. The complex device encrypts all the information between individual chips, or renders itself inoperable. Tamper resistance is generally used in packages in order to determine package or product tampering. Answer B is incorrect. Tamper evident specifies a process or device that makes unauthorized access to the protected object easily detected. Answer D is incorrect. Tamper proofing makes computers resistant to interference. Tamper proofing measures include automatic removal of

sensitive information, automatic shutdown, and automatic physical locking. Answer C is incorrect. Tamper data is used to view and modify the HTTP or HTTPS headers and post parameters.

NEW QUESTION: 23
What project management plan is most likely to direct the quantitative risk analysis process for a project in a matrix environment?
A. Risk analysis plan
B. Staffing management plan
C. Risk management plan
D. Human resource management plan
E. Explanation:
The risk management plan defines how risks will be identified, analyzed, responded to, and then monitored and controlled regardless of the structure of the organization.
F. is incorrect. The human resources management plan does define how risks will be analyzed.
G. is incorrect. The staffing management plan does define how risks will be analyzed.
Answer: C (LEAVE A REPLY)
is incorrect. The risk analysis plan does define how risks will be analyzed.

NEW QUESTION: 24
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: 25
Which of the following is a signature-based intrusion detection system (IDS) ?
A. RealSecure

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

NEW QUESTION: 26
A part of a project deals with the hardware work. As a project manager, you have decided to hire a company to deal with all hardware work on the project. Which type of risk response is this?
A. Exploit
B. Mitigation
C. Transference
D. Avoidance
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: When you are hiring a third party to own risk, it is known as transference risk response.
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. AnswerB is incorrect. The act of spending money to reduce a risk probability and impact is known as mitigation.
AnswerA is incorrect. Exploit is a strategy that may be selected for risks with positive impacts where the
organization wishes to ensure that the opportunity is realized. AnswerD is incorrect. When extra activities are introduced into the project to avoid the risk, this is an example of avoidance.

NEW QUESTION: 27
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)
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 Answer B is incorrect. This element is included in the ISO 27005 standard. Answer D is incorrect. This element is included in the ISO 27006 standard.

NEW QUESTION: 28
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: 29
Which of the following statements about the integrity concept of information security management are true? Each correct answer represents a complete solution. Choose three.

A. It ensures that unauthorized modifications are not made to data by authorized personnel or processes.
B. It determines the actions and behaviors of a single individual within a system
C. It ensures that internal information is consistent among all subentities and also consistent with the real- world, external situation.
D. It ensures that modifications are not made to data by unauthorized personnel or processes.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: The following statements about the integrity concept of information security management are true: It ensures that modifications are not made to data by unauthorized personnel or processes. It ensures that unauthorized modifications are not made to data by authorized personnel or processes. It ensures that internal information is consistent among all subentities and also consistent with the real-world, external situation. AnswerB is incorrect. Accountability determines the actions and behaviors of an individual within a system, and identifies that particular individual. Audit trails and logs support accountability.

NEW QUESTION: 30
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: 31
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: 32
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: 33
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)
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: 34
Adrian is the project manager of the NHP Project. In her project there are several work packages that deal with electrical wiring. Rather than to manage the risk internally she has decided to hire a vendor to complete all work packages that deal with the electrical wiring. By removing the risk internally to a licensed electrician Adrian feels more comfortable with project team being safe. What type of risk response has Adrian used in this example?
A. Acceptance
B. Avoidance
C. Mitigation

D. Transference

Answer: (SHOW ANSWER)

This is an example of transference. When the risk is transferred to a third party, usually for a fee, it creates a contractual-relationship for the third party to manage the risk on behalf of the performing organization. Risk response planning is a method of developing options to decrease the amount of threats and make the most of opportunities. The risk response should be aligned with the consequence of the risk and cost-effectiveness. This planning documents the processes for managing risk events. It addresses the owners and their responsibilities, risk identification, results from qualification and quantification processes, budgets and times for responses, and contingency plans. The various risk response planning techniques are as follows: Risk acceptance: It indicates that the project team has decided not to change the project management plan to deal with a risk, or is unable to identify any other suitable response strategy. Risk avoidance: It is a technique for a threat, which creates changes to the project management plan that are meant to either eliminate the risk or to protect the project objectives from this impact. Risk mitigation: It is a list of specific actions being taken to deal with specific risks associated with the threats and seeks to reduce the probability of occurrence or impact of risk below an acceptable threshold. Risk transference: It is used to shift the impact of a threat to a third party, together with the ownership of the response.

Topic 3, Volume C

NEW QUESTION: 35

Which of the following models uses a directed graph to specify the rights that a subject can transfer to an object or that a subject can take from another subject?

A. Take-Grant Protection Model

B. Biba Integrity Model

C. Bell-LaPadula Model

D. Access Matrix

Answer: A (LEAVE A REPLY)

The take-grant protection model is a formal model used in the field of computer security to establish or disprove the safety of a given computer system that follows specific rules. It shows that for specific systems the question of safety is decidable in linear time, which is in general undecidable. The model represents a system as directed graph, where vertices are either subjects or objects. The edges between them are labeled and the label indicates the rights that the source of the edge has over the destination. Two rights occur in every instance of the model: take and grant. They play a special role in the graph rewriting rules describing admissible changes of the graph. Answer D is incorrect. The access matrix is a straightforward approach that provides access rights to subjects for objects. Answer C is incorrect. The Bell-LaPadula model deals only with the confidentiality of classified material. It does not address integrity or availability. Answer B is incorrect. The integrity model was developed as an analog to the Bell-LaPadula confidentiality model and then became more sophisticated to address additional integrity requirements.

NEW QUESTION: 36
Which of the following security controls works as the totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy?
A. Common data security architecture (CDSA)
B. Application program interface (API)
C. Trusted computing base (TCB)
D. Internet Protocol Security (IPSec)
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: Trusted computing base (TCB) refers to hardware, software, controls, and processes that cause a computer system or network to be devoid of malicious software or hardware. Maintaining the trusted computing base (TCB) is essential for security policy to be implemented successfully. AnswerD is incorrect. Internet Protocol Security (IPSec) is a standard-based protocol that provides the highest level of VPN security. IPSec can encrypt virtually everything above the networking layer. It is used for VPN connections that use the L2TP protocol. It secures both data and password. IPSec cannot be used with Point-to-Point Tunneling Protocol (PPTP). Answer: A is incorrect. The Common data security architecture (CDSA) is a set of layered security services and cryptographic framework. It deals with the communications and data security problems in the emerging Internet and intranet application space. It presents an infrastructure for building cross-platform, interoperable, security-enabled applications for client-server environments. Answer: B is incorrect. An application programming interface (API) is an interface implemented by a software program which enables it to interact with other software. It facilitates interaction between different software programs similar to the way the user interface facilitates interaction between humans and computers. An API is implemented by applications, libraries, and operating systems to determine their vocabularies and calling conventions, and is used to access their services. It may include specifications for routines, data structures, object classes, and protocols used to communicate between the consumer and the implementer of the API.

NEW QUESTION: 37
Which of the following rated systems of the Orange book has mandatory protection of the TCB?
A. A-rated
B. B-rated
C. D-rated
D. C-rated
Answer: B (LEAVE A REPLY)
A B-rated system of the orange book has mandatory protection of the trusted computing base (TCB). Trusted computing base (TCB) refers to hardware, software, controls, and processes that

cause a computer system or network to be devoid of malicious software or hardware. Maintaining the trusted computing base (TCB) is essential for security policy to be implemented successfully.

NEW QUESTION: 38
Which of the following US Acts emphasized a "risk-based policy for cost-effective security" and makes mandatory for agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget?
A. Federal Information Security Management Act of 2002 (FISMA)
B. The Electronic Communications Privacy Act of 1986 (ECPA)
C. The Equal Credit Opportunity Act (ECOA)
D. The Fair Credit Reporting Act (FCRA)
Answer: (SHOW ANSWER)
Explanation/Reference:
The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. 3541, et seq.) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899). The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA has brought attention within the federal government to cybersecurity and explicitly emphasized a "risk-based policy for cost-effective security".
FISMA requires agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget (OMB).
OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act. Answer C is incorrect. The Equal Credit Opportunity Act (ECOA) is a United States law (codified at 15 U S C 1691 et seq), enacted in 1974, that makes it unlawful for any creditor to discriminate against any applicant, with respect to any aspect of a credit transaction, on the basis of race, color, religion, national origin, sex, marital status, or age; to the fact that all or part of the applicant's income derives from a public assistance program; or to the fact that the applicant has in good faith exercised any right under the Consumer Credit Protection Act. The law applies to any person who, in the ordinary course of business, regularly participates in a credit decision, including banks, retailers, bankcard companies, finance companies, and credit unions. Answer B is incorrect. The Electronic Communications Privacy Act of 1986 (ECPA Pub. L 99-508, Oct 21, 1986,
100 Stat. 1848, 18 U.S.C. 2510) was enacted by the United States Congress to extend government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer.

Specifically, ECPA was an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of
1968 (the Wiretap Statute), which was primarily designed to prevent unauthorized government access to private electronic communications. The ECPA also added new provisions prohibiting access to stored electronic communications, i.e., the Stored Communications Act,18 U.S.C. 2701-2712. AnswerD is incorrect. The Fair Credit Reporting Act (FCRA) is an American federal law (codified at 15 U.S.C. 1681 et seq.) that regulates the collection, dissemination, and use of consumer information, including consumer credit information. Along with the Fair Debt Collection Practices Act (FDCPA), it forms the base of consumer credit rights in the United States. It was originally passed in 1970, and is enforced by the US Federal Trade Commission.

NEW QUESTION: 39
Which of the following are included in Technical Controls? Each correct answer represents a complete solution. Choose all that apply.
A. Identification and authentication methods
B. Configuration of the infrastructure
C. Password and resource management
D. Implementing and maintaining access control mechanisms
E. Security devices
F. Conducting security-awareness training
Answer: (SHOW ANSWER)
Technical Controls are also known as Logical Controls. These controls include the following: Implementing and maintaining access control mechanisms Password and resource management Identification and authentication methods Security devices Configuration of the infrastructure Answer F is incorrect. It is a part of Administrative Controls.

NEW QUESTION: 40
Which of the following individuals inspects whether the security policies, standards, guidelines, and procedures are efficiently performed in accordance with the company's stated security objectives?
A. Information system security professional
B. Data owner
C. Senior management
D. Information system auditor
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation: An information system auditor is an individual who inspects whether the security policies, standards, guidelines, and procedures are efficiently performed in accordance with the company's stated security objectives. He is responsible for reporting the senior management about the value of security controls by performing regular and independent audits. Answer: B is incorrect. A data owner determines the sensitivity or classification levels of data. Answer: A is

incorrect. An informational systems security professional is an individual who designs, implements, manages, and reviews the security policies, standards, guidelines, and procedures of the organization. He is responsible to implement and maintain security by the senior-level management. Answer: C is incorrect. A senior management assigns overall responsibilities to other individuals.

NEW QUESTION: 41
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: D (LEAVE A REPLY)
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: 42
Which of the following rated systems of the Orange book has mandatory protection of the TCB?
A. A-rated
B. B-rated
C. D-rated
D. C-rated
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: A B-rated system of the orange book has mandatory protection of the trusted computing base (TCB).

Trusted computing base (TCB) refers to hardware, software, controls, and processes that cause a computer system or network to be devoid of malicious software or hardware. Maintaining the trusted computing base (TCB) is essential for security policy to be implemented successfully.

NEW QUESTION: 43
Which of the following are examples of the application programming interface (API)? Each correct answer represents a complete solution. Choose three.
A. HTML
B. PHP
C. .NET
D. Perl
Answer: B,C,D (LEAVE A REPLY)
Perl, .NET, and PHP are examples of the application programming interface (API). API is a set of routines, protocols, and tools that users can use to work with a component, application, or operating system. It consists of one or more DLLs that provide specific functionality. API helps in reducing the development time of applications by reducing application code. Most operating environments, such as MS-Windows, provide an API so that programmers can write applications consistent with the operating environment. Answer A is incorrect. HTML stands for Hypertext Markup Language. It is a set of markup symbols or codes used to create Web pages and define formatting specifications. The markup tells the Web browser how to display the content of the Web page.

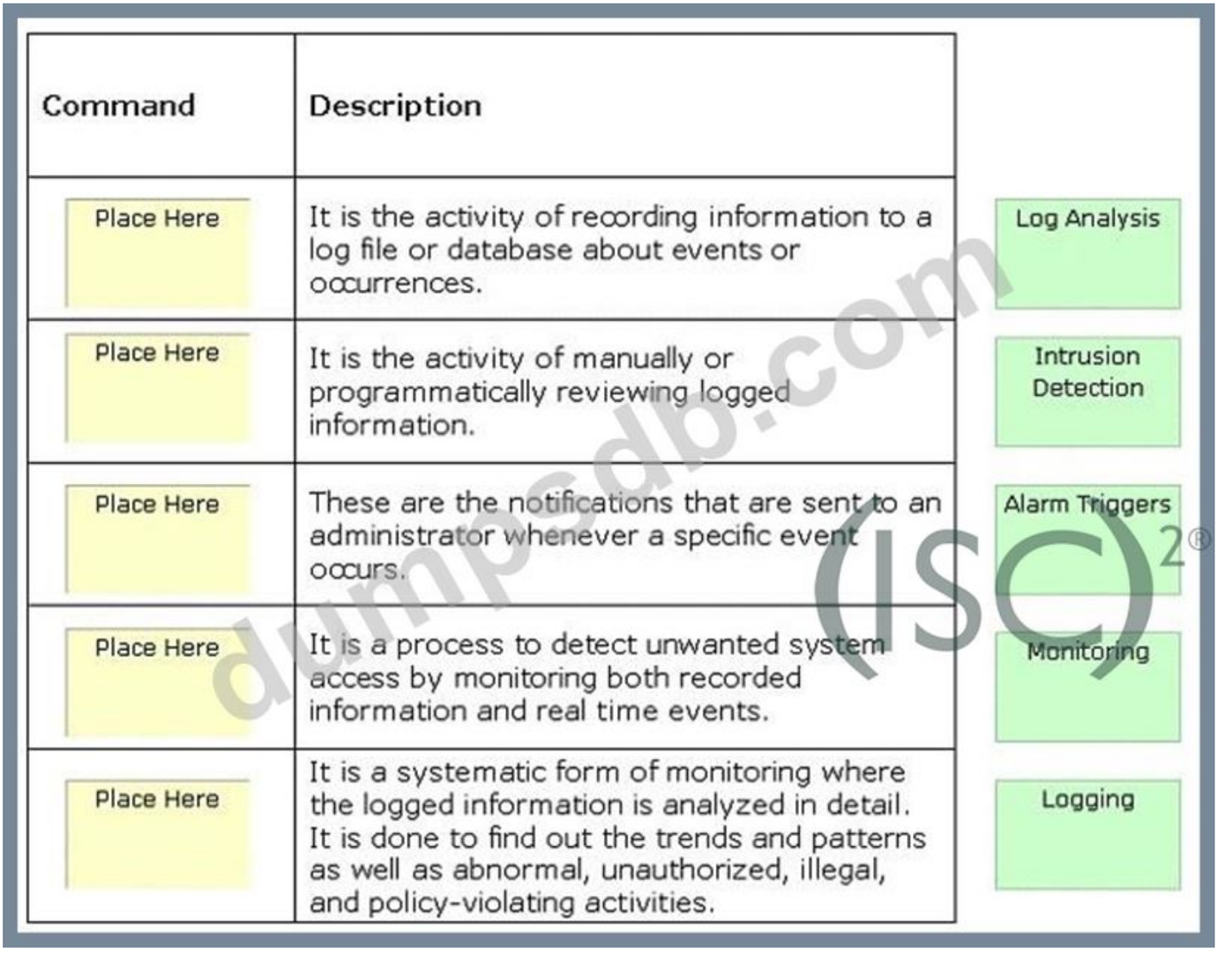
NEW QUESTION: 44
Which of the following allows multiple operating systems (guests) to run concurrently on a host computer?
A. Emulator
B. Hypervisor
C. Grid computing
D. CP/CMS
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: A hypervisor is a virtualization technique that allows multiple 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. AnswerA is incorrect. Emulator duplicates the functions of one system using a different system, so that the second system behaves like the first system. Answer D is incorrect. CP/CMS is a time-sharing operating system of the late 60s and early 70s, and it is known for its excellent performance and advanced features. Answer:
C is incorrect. Grid computing refers to the combination of computer resources from multiple administrative domains to achieve a common goal.

NEW QUESTION: 45

DRAG DROP

Auditing is used to track user accounts for file and object access, logon attempts, system shutdown, and many more vulnerabilities to enhance the security of the network. It encompasses a wide variety of activities. Place the different auditing activities in front of their descriptions.

Select and Place:



Answer:

Command	Description
Logging	It is the activity of recording information to a log file or database about events or occurrences.
Monitoring	It is the activity of manually or programmatically reviewing logged information.
Alarm Triggers	These are the notifications that are sent to an administrator whenever a specific event occurs.
Intrusion Detection	It is a process to detect unwanted system access by monitoring both recorded information and real time events.
Log Analysis	It is a systematic form of monitoring where the logged information is analyzed in detail. It is done to find out the trends and patterns as well as abnormal, unauthorized, illegal, and policy-violating activities.

Explanation/Reference:
Explanation: Auditing encompasses a wide variety of activities as follows: Logging: It is the activity of recording information to a log file or database about events or occurrences. Log Analysis: It is a systematic form of monitoring where the logged information is analyzed in detail. It is done to find out the trends and patterns as well as abnormal, unauthorized, illegal, and policy-violating activities. Intrusion Detection: It is a process to detect unwanted system access by monitoring both recorded information and real time events.
Alarm Triggers: These are the notifications that are sent to an administrator whenever a specific event occurs. Monitoring: It is the activity of manually or programmatically reviewing logged information.

NEW QUESTION: 46
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: 47
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: 48
Which of the following techniques is used to identify attacks originating from a botnet?
A. Passive OS fingerprinting
B. Recipient filtering
C. IFilter
D. BPF-based filter
Answer: A (LEAVE A REPLY)
Explanation/Reference:

Explanation: Passive OS fingerprinting can identify attacks originating from a botnet. Network Administrators can configure the firewall to take action on a botnet attack by using information obtained from passive OS fingerprinting. Passive OS fingerprinting (POSFP) allows the sensor to determine the operating system used by the hosts. The sensor examines the traffic flow between two hosts and then stores the operating system of those two hosts along with their IP addresses. In order to determine the type of operating system, the sensor analyzes TCP SYN and SYN ACK packets that are traveled on the network. The sensor computes the attack relevance rating to determine the relevancy of victim attack using the target host OS. After it, the sensor modifies the alert's risk rating or filters the alert for the attack.
Passive OS fingerprinting is also used to improve the alert output by reporting some information, such as victim OS, relevancy to the victim in the alert, and source of the OS identification.
AnswerD is incorrect. A BPF-based filter is used to limit the number of packets seen by tcpdump; this renders the output more usable on networks with a high volume of traffic. Answer: B is incorrect. Recipient filtering is used to block messages on the basis of whom they are sent to. Answer: C is incorrect. IFilters are used to extract contents from files that are crawled. IFilters also remove application-specific formatting before the content of a document is indexed by the search engine.

NEW QUESTION: 49
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)
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: 50

Which of the following ensures that a party to a dispute cannot deny the authenticity of their signature on a document or the sending of a message that they originated?

A. Confidentiality

B. OS fingerprinting

C. Reconnaissance

D. Non-repudiation

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation: Non-repudiation is a term that refers to the ability to ensure that a party to a dispute cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

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. Answer: A is incorrect.

Confidentiality is a mechanism that ensures that only the intended and authorized recipients are able to read data. The data is so encrypted that even if an unauthorized user gets access to it, he will not get any meaning out of it. Answer: C is incorrect. Reconnaissance is a term that refers to information gathering behaviors that aim to profile the organization, employees, network, and systems before an attack is performed efficiently. It is the first step in the process of intrusion and involves unauthorized discovery and mapping of systems, services, or vulnerabilities. These discovery and mapping techniques are commonly known as scanning and enumeration. Common tools, commands, and utilities used for scanning and enumeration include ping, telnet, nslookup, rpcinfo, File Explorer, finger, etc. Reconnaissance activities take place before performing a malicious attack. These activities are used to increase the probability of successful operation against the target, and to increase the probability of hiding the attacker's identity.

Answer B 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: 51

Which of the following techniques is used to identify attacks originating from a botnet?

A. Passive OS fingerprinting

B. Recipient filtering

C. IFilter

D. BPF-based filter

Answer: (SHOW ANSWER)

Passive OS fingerprinting can identify attacks originating from a botnet. Network Administrators can configure the firewall to take action on a botnet attack by using information obtained from

passive OS fingerprinting. Passive OS fingerprinting (POSFP) allows the sensor to determine the operating system used by the hosts. The sensor examines the traffic flow between two hosts and then stores the operating system of those two hosts along with their IP addresses. In order to determine the type of operating system, the sensor analyzes TCP SYN and SYN ACK packets that are traveled on the network. The sensor computes the attack relevance rating to determine the relevancy of victim attack using the target host OS. After it, the sensor modifies the alert's risk rating or filters the alert for the attack. Passive OS fingerprinting is also used to improve the alert output by reporting some information, such as victim OS, relevancy to the victim in the alert, and source of the OS identification. Answer D is incorrect. A BPF-based filter is used to limit the number of packets seen by tcpdump; this renders the output more usable on networks with a high volume of traffic. Answer B is incorrect. Recipient filtering is used to block messages on the basis of whom they are sent to. Answer C is incorrect. IFilters are used to extract contents from files that are crawled. IFilters also remove application-specific formatting before the content of a document is indexed by the search engine.

NEW QUESTION: 52
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)
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: 53
Which of the following are the phases of the Certification and Accreditation (C&A) process? Each correct answer represents a complete solution. Choose two.
A. Continuous Monitoring
B. Auditing
C. Detection
D. Initiation
Answer: A,D (LEAVE A REPLY)
Explanation/Reference:
Explanation: The Certification and Accreditation (C&A) process consists of four distinct phases: 1.Initiation
2.Security Certification 3.Security Accreditation 4.Continuous Monitoring The C&A activities can be applied to an information system at appropriate phases in the system development life cycle

by selectively tailoring the various tasks and subtasks. AnswerB and C are incorrect. Auditing and detection are not phases of the Certification and Accreditation process.

NEW QUESTION: 54
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)
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: 55
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: 56
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: 57
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: 58
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. Which of the following participants are required in a NIACAP security assessment? Each correct answer represents a part of the solution. Choose all that apply.
A. Certification agent
B. Designated Approving Authority
C. IS program manager
D. Information Assurance Manager
E. User representative
Answer: A,B,C,E (LEAVE A REPLY)

The NIACAP roles are nearly the same as the DITSCAP roles. Four minimum participants (roles) are required to perform a NIACAP security assessment: IS program manager: The IS program manager is the primary authorization advocate. He is responsible for the Information Systems (IS) throughout the life cycle of the system development. Designated Approving Authority (DAA): 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. Certification agent: The certification agent is also referred to as the certifier. He provides the technical expertise to conduct the certification throughout the system life cycle. User representative: The user representative focuses on system availability, access, integrity, functionality, performance, and confidentiality in a Certification and Accreditation (C&A) process. Answer D is incorrect. Information Assurance Manager (IAM) is one of the key participants in the DIACAP process.

NEW QUESTION: 59
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: 60

Digital rights management (DRM) consists of compliance and robustness rules. Which of the following features does the robustness rule have? Each correct answer represents a complete solution. Choose three.

A. It specifies the various levels of robustness that are needed for asset security.

B. It specifies minimum techniques for asset security.

C. It specifies the behaviors of the DRM implementation and applications accessing the implementation.

D. It contains assets, such as device key, content key, algorithm, and profiling data.

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

The DRM (digital rights management) technology includes the following rules: 1.Compliance rule: This rule specifies the behaviors of the DRM implementation, and 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 2.Robustness rule: This rule has the following features: It specifies the various levels of robustness that are needed for asset security. It contains assets, such as device key, content key, algorithm, and profiling data. It specifies minimum techniques for asset security.

NEW QUESTION: 61

A service provider guarantees for end-to-end network traffic performance to a customer. Which of the following types of agreement is this?

A. SLA

B. VPN

C. NDA

D. LA

Answer: A (LEAVE A REPLY)

This is a type of service-level agreement. A service-level agreement (SLA) is a negotiated agreement between two parties where one is the customer and the other is the service provider. It records a common understanding about services, priorities, responsibilities, guarantees, and warranties. Each area of service scope should have the 'level of service' defined. The SLA may specify the levels of availability, serviceability, performance, operation, or other attributes of the service, such as billing. Answer C is incorrect. Non-disclosure agreements (NDAs) are often used to protect the confidentiality of an invention as it is being evaluated by potential licensees. Answer D is incorrect. License agreements (LA) describe the rights and responsibilities of a party related to the use and exploitation of intellectual property. Answer B is incorrect. There is no such type of agreement as VPN.

NEW QUESTION: 62
Which of the following methods does the Java Servlet Specification v2.4 define in the HttpServletRequest interface that control programmatic security? Each correct answer represents a complete solution. Choose all that apply.
A. getCallerIdentity()
B. isUserInRole()
C. getUserPrincipal()
D. getRemoteUser()
Answer: B,C,D (LEAVE A REPLY)
The various methods of the HttpServletRequest interface are as follows: getRemoteUser(): It returns the user name that is used for the client authentication. The value of the getRemoteUser() method returns null if no user is authenticated. isUserInRole(): It 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. getUserPrincipal(): It 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 A is incorrect. It is not defined in the HttpServletRequest interface. The getCallerIdentity() method is used to obtain the java.security.Identity of the caller.

NEW QUESTION: 63
In which of the following testing methodologies do assessors use all available documentation and work under no constraints, and attempt to circumvent the security features of an information system?
A. Full operational test
B. Penetration test
C. Paper test
D. Walk-through test
Answer: B (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. Answer: C is incorrect. A paper test is the least complex test in the disaster recovery and business continuity testing approaches. In this test, the BCP/DRP plan documents are distributed to the appropriate managers and BCP/DRP team members for review, markup, and comment. This approach helps the auditor to ensure that the plan is complete and that all team members are familiar with their responsibilities within the plan. Answer: D is incorrect. A walk-through test is an extension of the paper testing in the business continuity and disaster recovery process. In this testing methodology, appropriate managers and BCP/DRP team members discuss and walk through procedures of the plan. They also discuss the training needs, and clarification of critical plan elements. Answer: A is incorrect. A full operational test includes all team members and participants in the disaster recovery and business continuity process. This full operation test involves the mobilization of personnel. It restores operations in the same manner as an outage or disaster would. The full operational test extends the preparedness test by including actual notification, mobilization of resources, processing of data, and utilization of backup media for restoration.

NEW QUESTION: 64
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: 65
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: (SHOW ANSWER)

Explanation/Reference:

Explanation: The Industrial Property law and the Copyright law are the components of the Intellectual Property law.

NEW QUESTION: 66

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: A,B,C,D,E (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 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: 67

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)

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. Answer D 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. Answer A 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 Answer C 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: 68
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)
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: 69
Which of the following security issues does the Bell-La Padula model focus on?
A. Authorization
B. Confidentiality
C. Integrity
D. Authentication
Answer: B (LEAVE A REPLY)
The Bell-La Padula model is a state machine model used for enforcing access control in large organizations. It focuses on data confidentiality and access to classified information, in contrast to the Biba Integrity model, which describes rules for the protection of data integrity. In the Bell-La Padula model, the entities in an information system are divided into subjects and objects. The Bell-La Padula model is built on the concept of a state machine with a set of allowable states in a computer network system. The transition from one state to another state is defined by transition functions. The model defines two mandatory access control (MAC) rules and one discretionary access control (DAC) rule with three security properties: 1.The Simple Security Property: A subject at a given security level may not read an object at a higher security level (no read-up). 2.The *-property (star-property): A subject at a given security level must not write to any object at a lower security level (no write-down). The *-property is also known as the Confinement property. 3.The Discretionary Security Property: It uses an access matrix to specify the discretionary access control.

NEW QUESTION: 70
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: 71
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: 72
Which of the following is designed to detect unwanted attempts at accessing, manipulating, and disabling of computer systems through the Internet?
A. DAS
B. IPsec
C. IDS
D. ACL
Answer: C (LEAVE A REPLY)
Explanation/Reference:

Explanation: An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers, malware and/or disgruntled employees. An IDS cannot directly detect attacks within properly encrypted traffic. An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, trojan horses, and worms). Answer: D is incorrect. Access Control List (ACL) is the most commonly used object in Cisco IOS. It filters packets or network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. According to the criteria specified within the access lists, router determines whether the packets to be forwarded or dropped. Access control list criteria could be the source or destination address of the traffic or other information. The types of Cisco ACLs are Standard IP, Extended IP, IPX, Appletalk, etc. Answer: B is incorrect. Internet Protocol Security (IPSec) is a method of securing data. It secures traffic by using encryption and digital signing. It enhances the security of data as if an IPSec packet is captured, its contents cannot be read. IPSec also provides sender verification that ensures the certainty of the datagram's origin to the receiver. Answer: A is incorrect. Direct-attached storage (DAS) is a digital storage system that is directly attached to a server or workstation, without using a storage network.

NEW QUESTION: 73

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: 74
Maria has been recently appointed as a Network Administrator in Gentech Inc. She has been tasked to perform network security testing to find out the vulnerabilities and shortcomings of the present network infrastructure. Which of the following testing approaches will she apply to accomplish this task?
A. Gray-box testing
B. White-box testing
C. Black-box testing
D. Unit testing
Answer: C (LEAVE A REPLY)
Maria is new for this organization and she does not have any idea regarding the present infrastructure. Therefore, black box testing is best suited for her. Blackbox testing is a technique in which the testing team has no knowledge about the infrastructure of the organization. The testers must first determine the location and extent of the systems before commencing their analysis. This testing technique is costly and time consuming. Answer B is incorrect. White box testing, also known as Clear box or Glass box testing, takes into account the internal mechanism of a system or application. The connotations of "Clear box" and "Glass box" indicate that a tester has full visibility of the internal workings of the system. It uses knowledge of the internal structure of an application. It is applicable at the unit, integration, and system levels of the software testing process. It consists of the following testing methods: Control flow-based testing Create a graph from source code. Describe the flow of control through the control flow graph. Design test cases to cover certain elements of the graph. Data flow-based testing Test connections between variable definitions. Check variation of the control flow graph. Set DEF (n) contains variables that are defined at node n. Set USE (n) are variables that are read. Answer A is incorrect. 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 D 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: 75

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: 76

Copyright holders, content providers, and manufacturers use digital rights management (DRM) in order to limit usage of digital media and devices. Which of the following security challenges does DRM include? Each correct answer represents a complete solution. Choose all that apply.

A. OTA provisioning

B. Access control

C. Key hiding

D. Device fingerprinting

Answer: (SHOW ANSWER)

The security challenges for DRM are as follows: Key hiding: It prevents tampering attacks that target the secret keys. In the key hiding process, secret keys are used for authentication, encryption, and node-locking. Device fingerprinting: It prevents fraud and provides secure authentication. Device fingerprinting includes the summary of hardware and software characteristics in order to uniquely identify a device. OTA provisioning: It provides end-to-end encryption or other secure ways for delivery of copyrighted software to mobile devices. Answer B is incorrect. Access control is not a security challenge for DRM.

NEW QUESTION: 77
Which of the following allows multiple operating systems (guests) to run concurrently on a host computer?
A. Emulator
B. Hypervisor
C. Grid computing
D. CP/CMS
Answer: B (LEAVE A REPLY)
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 A is incorrect. Emulator duplicates the functions of one system using a different system, so that the second system behaves like the first system. Answer D is incorrect. CP/CMS is a time-sharing operating system of the late 60s and early 70s, and it is known for its excellent performance and advanced features. Answer C is incorrect. Grid computing refers to the combination of computer resources from multiple administrative domains to achieve a common goal.

NEW QUESTION: 78
The build environment of secure coding consists of some tools that actively support secure specification, design, and implementation. Which of the following features do these tools have? Each correct answer represents a complete solution. Choose all that apply.
A. They decrease the exploitable flaws and weaknesses.
B. They reduce and restrain the propagation, extent, and damage that have occurred by insecure software behavior.
C. They decrease the attack surface.
D. They employ software security constraints, protections, and services.
E. They decrease the level of type checking and program analysis.
Answer: A,B,C,D (LEAVE A REPLY)
The tools that produce secure software have the following features: They decrease the exploitable flaws and weaknesses. They decrease the attack surface. They employ software security constraints, protections, and services. They reduce and restrain the propagation, extent, and damage that are caused by the behavior of insecure software. Answer E is incorrect. This feature is not required for these tools.

NEW QUESTION: 79

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: 80

You are the project manager of the CUL project in your organization. You and the project team are assessing the risk events and creating a probability and impact matrix for the identified risks. Which one of the following statements best describes the requirements for the data type used in qualitative risk analysis?

A. A qualitative risk analysis encourages biased data to reveal risk tolerances.

B. A qualitative risk analysis required unbiased stakeholders with biased risk tolerances.

C. A qualitative risk analysis requires accurate and unbiased data if it is to be credible.

D. A qualitative risk analysis requires fast and simple data to complete the analysis.

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation: Of all the choices only this answer is accurate. The PMBOK clearly states that the data must be accurate and unbiased to be credible. Answer: D is incorrect. This is not a valid statement about the qualitative risk analysis data. Answer: A is incorrect. This is not a valid

statement about the qualitative risk analysis data. Answer: B is incorrect. This is not a valid statement about the qualitative risk analysis data.

NEW QUESTION: 81
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: 82
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)
Explanation/Reference:
Explanation: 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: 83

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: 84

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)

Explanation/Reference:

Explanation: 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.

AnswerD 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. AnswerA 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. AnswerB 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: 85
Which of the following fields of management focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life?
A. Configuration management
B. Risk management
C. Change management
D. Procurement management
Answer: A (LEAVE A REPLY)
Configuration management is a field of management that focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life. 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 D is incorrect. The procurement management plan defines more than just the procurement of team members, if needed. It defines how procurements will be planned and executed, and how the organization and the vendor will fulfill the terms of the contract. Answer B is incorrect. Risk Management is used to identify, assess, and control risks. It includes analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats. Answer C is incorrect. Change Management is used to ensure that standardized methods and procedures are used for efficient handling of all changes.

NEW QUESTION: 86
Which of the following are the important areas addressed by a software system's security policy? Each correct answer represents a complete solution. Choose all that apply.
A. Identification and authentication
B. Punctuality
C. Data protection
D. Accountability
E. Scalability
F. Access control
Answer: A,C,D,F (LEAVE A REPLY)
The security policy of a software system addresses the following important areas: Access control Data protection Confidentiality Integrity Identification and authentication Communication security Accountability Answer E and B are incorrect. Scalability and punctuality are not addressed by a software system's security policy.

NEW QUESTION: 87
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: 88
In which of the following processes are experienced personnel and software tools used to investigate, resolve, and handle process deviation, malformed data, infrastructure, or connectivity issues?
A. Risk Management
B. Exception management

C. Configuration Management
D. Change Management
E. Explanation:
Exception management is a process in which experienced personnel and software tools are used to investigate, resolve, and handle process deviation, malformed data, infrastructure or connectivity issues. It increases the efficiency of business processes and contributes in the progress of business.
Answer: (SHOW ANSWER)
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. Answer A is incorrect. Risk Management is used to identify, assess, and control risks. It includes analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats. Risk Management is part of Service Design and the owner of the Risk Management is the Risk Manager. Risks are addressed within several processes in ITIL V3; however, there is no dedicated Risk Management process. ITIL V3 calls for "coordinated risk assessment exercises", so at IT Process Maps we decided to assign clear responsibilities for managing risks. Answer D is incorrect. Change Management is used to ensure that standardized methods and procedures are used for efficient handling of all changes. A change is "an event that results in a new status of one or more configuration items (CI's)" approved by management, cost effective, enhances business process changes (fixes) - with a minimum risk to IT infrastructure. The main aims of Change Management are as follows: Minimal disruption of services Reduction in back-out activities Economic utilization of resources involved in the change

NEW QUESTION: 89
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: (SHOW ANSWER)
Explanation/Reference:
Explanation: 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 AnswerD 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: 90
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: (SHOW ANSWER)
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: 91
Which of the following is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known, but by which a business can obtain an economic advantage over its competitors?
A. Copyright
B. Utility model
C. Trade secret
D. Cookie
E. Explanation:
A trade secret is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known. It helps a business to obtain an economic advantage

over its competitors or customers. In some jurisdictions, such secrets are referred to as confidential information or classified information.

Answer: C (LEAVE A REPLY)

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. A utility model is an intellectual property right to protect inventions. Answer D is incorrect. A cookie is a small bit of text that accompanies requests and pages as they move between Web servers and browsers. It contains information that is read by a Web application, whenever a user visits a site. Cookies are stored in the memory or hard disk of client computers. A Web site stores information, such as user preferences and settings in a cookie. This information helps in providing customized services to users. There is absolutely no way a Web server can access any private information about a user or his computer through cookies, unless a user provides the information. A Web server cannot access cookies created by other Web servers.

NEW QUESTION: 92

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)

Explanation/Reference:

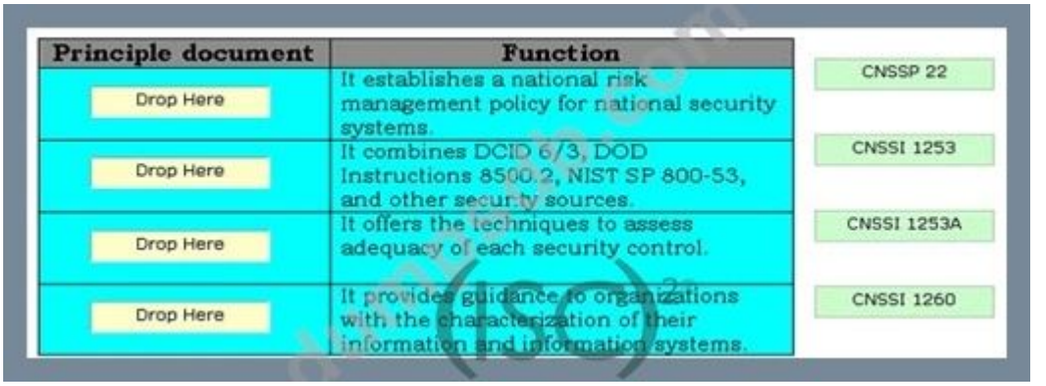
Explanation: ISO 27004 is an information security standard developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is entitled as "Information technology - Security techniques - Information security management - Measurement". The 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. AnswerA 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".

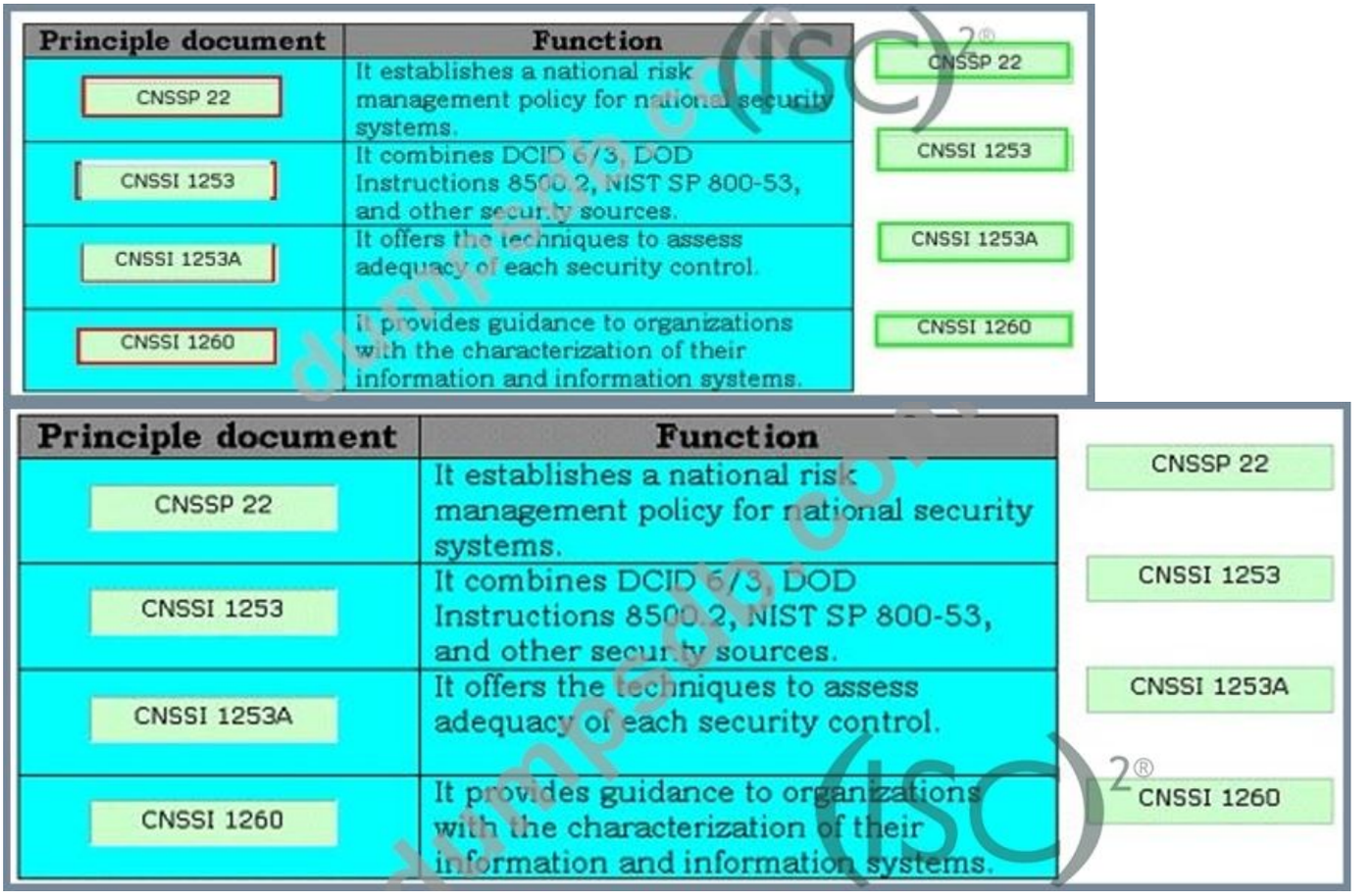
NEW QUESTION: 93

DRAG DROP

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



Answer:



The various principle documents of transformation are as follows: CNSSP 22: It establishes a national risk management policy for national security systems. CNSSI 1199: It creates the

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

NEW QUESTION: 94
Samantha works as an Ethical Hacker for we-are-secure Inc. She wants to test the security of the we-are- secure server for DoS attacks. She sends large number of ICMP ECHO packets to the target computer.
Which of the following DoS attacking techniques will she use to accomplish the task?
A. Smurf dos attack
B. Land attack
C. Ping flood attack
D. Teardrop attack
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: According to the scenario, Samantha is using the ping flood attack. In a ping flood attack, an attacker sends a large number of ICMP packets to the target computer using the ping command, i.e., ping - f target_IP_address. When the target computer receives these packets in large quantities, it does not respond and hangs. However, for such an attack to take place, the attacker must have sufficient Internet bandwidth, because if the target responds with an "ECHO reply ICMP packet" message, the attacker must have both the incoming and outgoing bandwidths available for communication. AnswerA is incorrect. In a smurf DoS attack, an attacker sends a large amount of ICMP echo request traffic to the IP broadcast addresses. These ICMP requests have a spoofed source address of the intended victim. If the routing device delivering traffic to those broadcast addresses delivers the IP broadcast to all the hosts, most of the IP addresses send an ECHO reply message. However, on a multi- access broadcast network, hundreds of computers might reply to each packet when the target network is overwhelmed by all the messages sent simultaneously. Due to this, the network becomes unable to provide services to all the messages and crashes. Answer D is incorrect. In a teardrop attack, a series of data packets are sent to the target computer with overlapping offset field values. As a result, the target computer is unable to reassemble these packets and is forced to crash, hang, or reboot. Answer: B is incorrect. In a land attack, the attacker sends a spoofed TCP SYN packet in which the IP address of the target is filled in both the source and destination fields. On receiving the spoofed packet, the target system becomes confused and goes into a frozen state. Now-a-days, antivirus can easily detect such an attack.

NEW QUESTION: 95
Which of the following models manages the software development process if the developers are limited to go back only one stage to rework?
A. Waterfall model
B. Spiral model
C. RAD model
D. Prototyping model
Answer: A (LEAVE A REPLY)
In the waterfall model, software development can be managed if the developers are limited to go back only one stage to rework. If this limitation is not imposed mainly on a large project with several team members, then any developer can be working on any phase at any time, and the required rework might be accomplished several times. Answer B is incorrect. The spiral model is a software development process combining elements of both design and prototyping-instages, in an effort to combine advantages of top-down and bottom-up concepts. The basic principles of the spiral model are as follows: The focus is on risk assessment and minimizing project risks by breaking a project into smaller segments and providing more ease-of- change during the development process, as well as providing the opportunity to evaluate risks and weigh consideration of project continuation throughout the life cycle. Each cycle involves a progression through the same sequence of steps, for each portion of the product and for each of its levels of elaboration, from an overall concept-of-operation document down to the coding of each individual program. Each trip around the spiral traverses the following four basic quadrants: Determine objectives, alternatives, and constraints of the iteration. Evaluate alternatives, and identify and resolve risks. Develop and verify deliverables from the iteration. Plan the next iteration. Begin each cycle with an identification of stakeholders and their win conditions, and end each cycle with review and commitment. Answer D is incorrect. The Prototyping model is a systems development method (SDM). In this model, a prototype is created, tested, and then reworked as necessary until an adequate prototype is finally achieved from which the complete system or product can now be developed. Answer C is incorrect. Rapid Application Development (RAD) refers to a type of software development methodology that uses minimal planning in favor of rapid prototyping.

NEW QUESTION: 96
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)
Explanation/Reference:

Explanation: 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. AnswerD 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. AnswerC 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. AnswerA 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: 97
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: 98

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: 99

Gary is the project manager for his project. He and the project team have completed the qualitative risk analysis process and are about to enter the quantitative risk analysis process when Mary, the project sponsor, wants to know what quantitative risk analysis will review. Which of the following statements best defines what quantitative risk analysis will review?

A. The quantitative risk analysis process will analyze the effect of risk events that may substantially impact the project's competing demands.

B. The quantitative risk analysis reviews the results of risk identification and prepares the project for risk response management.

C. The quantitative risk analysis seeks to determine the true cost of each identified risk event and the probability of each risk event to determine the risk exposure.

D. The quantitative risk analysis process will review risk events for their probability and impact on the project objectives.

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Once the risk events have passed through qualitative risk analysis, then the risk events must be reviewed to determine the effect of the risks on the project's competing demands. Answer D is incorrect. While the quantitative risk analysis process will review the risk events for probability and impact, this statement does not answer the question as completely as answer option A Answer C is incorrect. The quantitative risk analysis process does not review every risk identified - only the risks which require further analysis. AnswerB is incorrect. Quantitative risk analysis process does not begin the risk response process. Its goal is to determine the effect of certain risk events on the project's competing demands.

NEW QUESTION: 100

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: A (LEAVE A REPLY)
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: 101
DRAG DROP
Drag and drop the various SSE-CMM levels at the appropriate places.

DESCRIPTION	LEVEL
It focuses on whether an organization or project performs a process that incorporates the BPs.	Drop Here
It focuses on project-level definition, planning, and performance issues.	Drop Here
It focuses on disciplined tailoring from defined processes at the organization level.	Drop Here
It gains leverage from all the management practice improvements seen in the earlier levels, then emphasizes the cultural shifts that will sustain the gains made.	Drop Here

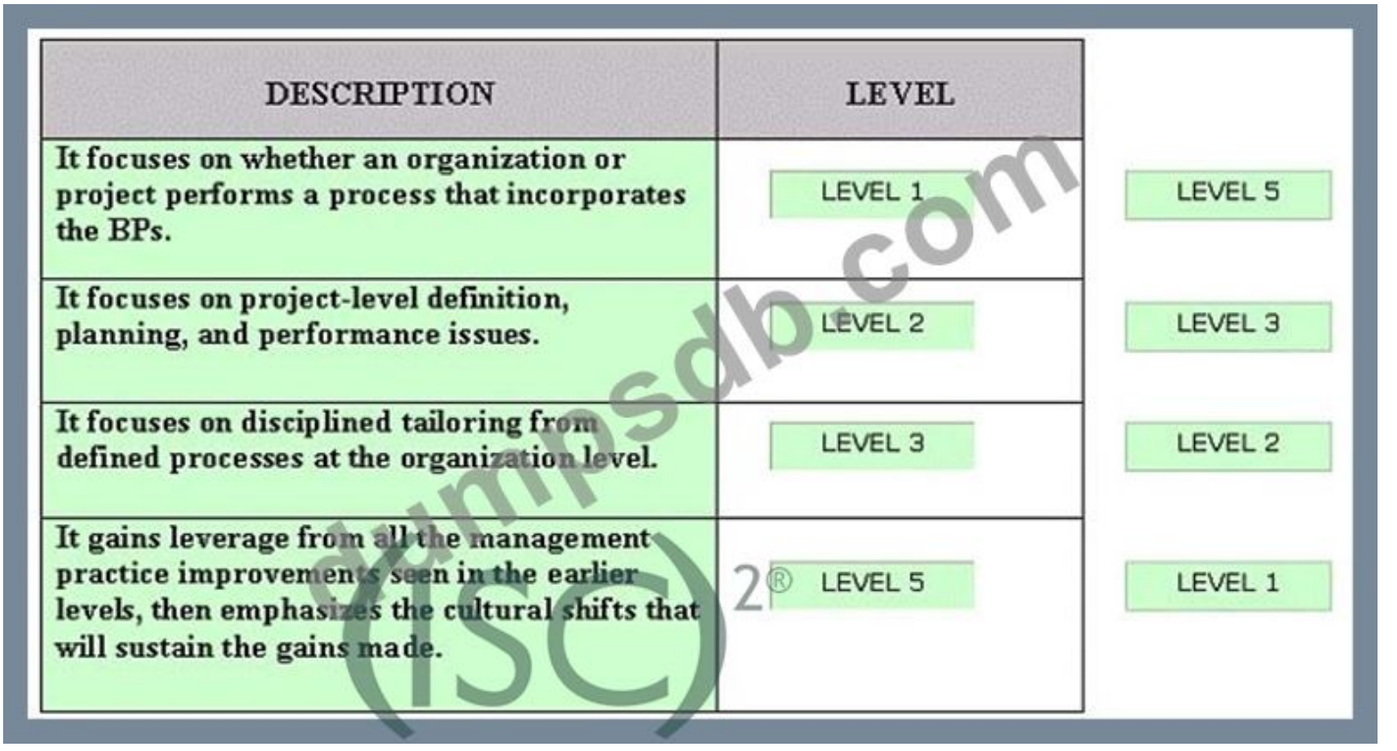
LEVEL 5
LEVEL 3
LEVEL 2
LEVEL 1

Answer:

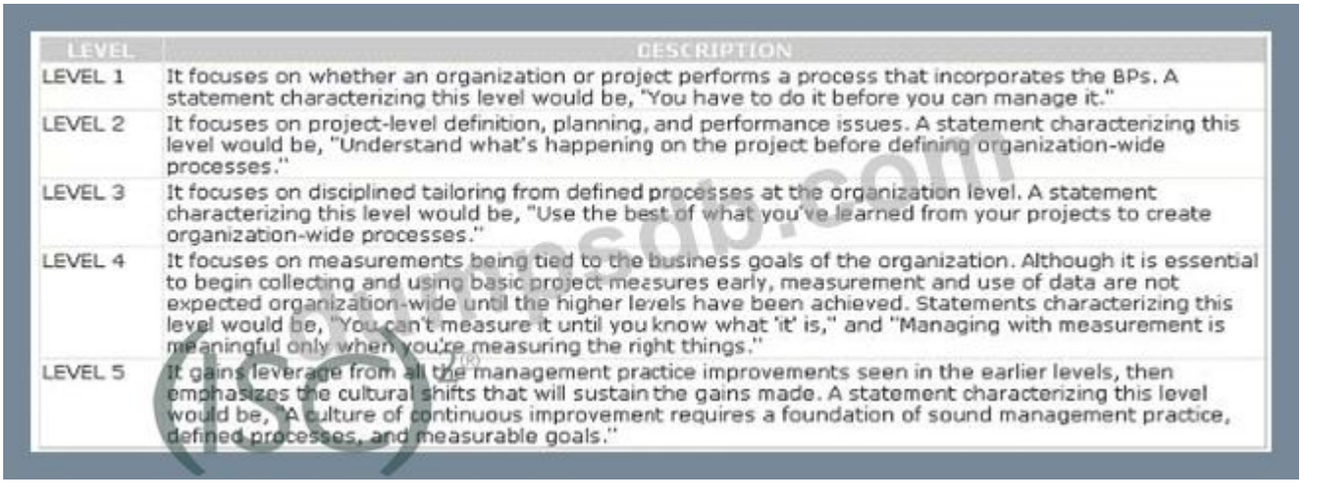
DESCRIPTION	LEVEL
It focuses on whether an organization or project performs a process that incorporates the BPs.	LEVEL 1
It focuses on project-level definition, planning, and performance issues.	LEVEL 2
It focuses on disciplined tailoring from defined processes at the organization level.	LEVEL 3
It gains leverage from all the management practice improvements seen in the earlier levels, then emphasizes the cultural shifts that will sustain the gains made.	LEVEL 5

LEVEL 5
LEVEL 3
LEVEL 2
LEVEL 1

Explanation:



The various SSE-CMM levels are described in the table below:



LEVEL	DESCRIPTION
LEVEL 1	It focuses on whether an organization or project performs a process that incorporates the BPs. A statement characterizing this level would be, "You have to do it before you can manage it."
LEVEL 2	It focuses on project-level definition, planning, and performance issues. A statement characterizing this level would be, "Understand what's happening on the project before defining organization-wide processes."
LEVEL 3	It focuses on disciplined tailoring from defined processes at the organization level. A statement characterizing this level would be, "Use the best of what you've learned from your projects to create organization-wide processes."
LEVEL 4	It focuses on measurements being tied to the business goals of the organization. Although it is essential to begin collecting and using basic project measures early, measurement and use of data are not expected organization-wide until the higher levels have been achieved. Statements characterizing this level would be, "You can't measure it until you know what 'it' is," and "Managing with measurement is meaningful only when you're measuring the right things."
LEVEL 5	It gains leverage from all the management practice improvements seen in the earlier levels, then emphasizes the cultural shifts that will sustain the gains made. A statement characterizing this level would be, "A culture of continuous improvement requires a foundation of sound management practice, defined processes, and measurable goals."

NEW QUESTION: 102
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: (SHOW ANSWER)
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: 103
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)
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: 104
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: 105
Which of the following security models dictates that subjects can only access objects through applications?
A. Biba model
B. Bell-LaPadula
C. Clark-Wilson
D. Biba-Clark model
Answer: C (LEAVE A REPLY)
The Clark-Wilson security model dictates that subjects can only access objects through applications. Answer A is incorrect. The Biba model does not let subjects write to objects at a higher integrity level. Answer B is incorrect. The Bell-LaPadula model has a simple security rule, which means a subject cannot read data from a higher level. Answer D is incorrect. There is no such model as Biba-Clark model.

NEW QUESTION: 106
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 are tested and reviewed?
A. Level 4
B. Level 5
C. Level 2
D. Level 3
E. Level 1
Answer: A (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: 107
Which of the following types of attacks occurs when an attacker successfully inserts an intermediary software or program between two communicating hosts?
A. Denial-of-service attack
B. Dictionary attack
C. Man-in-the-middle attack
D. Password guessing attack
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: When an attacker successfully inserts an intermediary software or program between two communicating hosts, it is known as man-in-the-middle attack.

NEW QUESTION: 108
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)
Explanation/Reference:
Explanation: 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: 109
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)
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: 110
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: (SHOW ANSWER)
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: 111
The LeGrand Vulnerability-Oriented Risk Management method is based on vulnerability analysis and consists of four principle steps. Which of the following processes does the risk assessment step include? Each correct answer represents a part of the solution. Choose all that apply.
A. Remediation of a particular vulnerability
B. Cost-benefit examination of countermeasures
C. Identification of vulnerabilities
D. Assessment of attacks
Answer: B,C,D (LEAVE A REPLY)

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

NEW QUESTION: 112
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: (SHOW ANSWER)
Explanation/Reference:
Explanation: 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: 113
Which of the following disaster recovery tests includes the operations that shut down at the primary site, and are shifted to the recovery site according to the disaster recovery plan?
A. Structured walk-through test
B. Full-interruption test
C. Parallel test
D. Simulation test
Answer: (SHOW ANSWER)
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. Answer A 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 C 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. Answer D is incorrect. 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.

NEW QUESTION: 114
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)
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: 115
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: A,B,C,E (LEAVE A REPLY)
Explanation/Reference:
Explanation: The service-oriented modeling framework (SOMF) concentrates on the following principles:

Business traceability Architectural best-practices traceability Technological traceability SOA value proposition Software assets reuse SOA integration strategies Technological abstraction and generalization Architectural components abstraction Answer: D is incorrect. The service-oriented modeling framework (SOMF) does not concentrate on it.

NEW QUESTION: 116
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)
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: 117
In digital rights management, the level of robustness depends on the various types of tools and attacks to which they must be resistant or immune. Which of the following types of tools are expensive, require skill, and are not easily available?
A. Hand tools
B. Widely available tools
C. Specialized tools
D. Professional tools
Answer: D (LEAVE A REPLY)
The tools used in DRM to define the level of robustness are as follows: 1.Widely available tools: These tools are easy to use and are available to everyone. For example, screwdrivers and file editors. 2.Specialized tools: These tools require skill and are available at reasonable prices. For example, debuggers, decompilers, and memory scanners. 3.Professional tools: These tools are expensive, require skill, and are not easily available. For example, logic analyzers, circuit emulators, and chip disassembly systems.

NEW QUESTION: 118
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)
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: 119
You work as a security engineer for BlueWell Inc. You want to use some techniques and procedures to verify the effectiveness of security controls in Federal Information System. Which of the following NIST documents will guide you?
A. NIST Special Publication 800-53
B. NIST Special Publication 800-59
C. NIST Special Publication 800-53A
D. NIST Special Publication 800-37
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: NIST has developed a suite of documents for conducting Certification & Accreditation (C&A).
These documents are as follows: 1.NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems. 2.NIST Special Publication 800-53:
This document provides a guideline for security controls for Federal Information Systems. 3.NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System. 4.NIST Special Publication 800-59: This document provides a guideline for identifying an information system as a National Security System. 5.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: 120

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: (SHOW ANSWER)

Explanation/Reference:

Explanation: 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. AnswerD is incorrect. Virtualization increases configuration effort because of complexity of the virtualization layer and composite system.

NEW QUESTION: 121

Microsoft software security expert Michael Howard defines some heuristics for determining code review in "A Process for Performing Security Code Reviews". Which of the following heuristics increase the application's attack surface? Each correct answer represents a complete solution. Choose all that apply.

A. Code written in C/C++/assembly language

B. Code listening on a globally accessible network interface

C. Code that changes frequently

D. Anonymously accessible code

E. Code that runs by default

F. Code that runs in elevated context

Answer: (SHOW ANSWER)

Microsoft software security expert Michael Howard defines the following heuristics for determining code review in "A Process for Performing Security Code Reviews": Old code: Newer code provides better understanding of software security and has lesser number of vulnerabilities. Older code must be checked deeply. Code that runs by default: It must have high quality, and must be checked deeply than code that does not execute by default. Code that runs by default increases the application's attack surface. Code that runs in elevated context: It must have higher quality. Code that runs in elevated privileges must be checked deeply and increases the application's attack surface. Anonymously accessible code: It must be checked deeply than code that only authorized users and administrators can access, and it increases the application's attack surface. Code listening on a globally accessible network interface: It must be checked deeply for security vulnerabilities and increases the application's attack surface. Code written in C/C++/assembly language: It is prone to security vulnerabilities, for example, buffer overruns. Code with a history of security vulnerabilities: It includes additional vulnerabilities except concerted efforts that are

required for removing them. Code that handles sensitive data: It must be checked deeply to ensure that data is protected from unintentional disclosure. Complex code: It includes undiscovered errors because it is more difficult to analyze complex code manually and programmatically. Code that changes frequently: It has more security vulnerabilities than code that does not change frequently.

NEW QUESTION: 122
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: 123

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: 124

You work as a Security Manager for Tech Perfect Inc. You have set up a SIEM server for the following purposes: Analyze the data from different log sources Correlate the events among the log entries Identify and prioritize significant events Initiate responses to events if required One of your log monitoring staff wants to know the features of SIEM product that will help them in these purposes. What features will you recommend? Each correct answer represents a complete solution. Choose all that apply.

A. Asset information storage and correlation

B. Transmission confidentiality protection

C. Incident tracking and reporting

D. Security knowledge base

E. Graphical user interface

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation: The features of SIEM products are as follows: Graphical user interface (GUI): It is used in analysis for identifying potential problems and reviewing all available data that are

associated with the problems. Security knowledge base: It includes information on known vulnerabilities, log messages, and other technical data. Incident tracking and hacking: It has robust workflow features to track and report incidents. Asset information storage and correlation: It gives higher priority to an attack that affects a vulnerable OS or a main host. Answer: B is incorrect. SIEM product does not have this feature.

NEW QUESTION: 125
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: 126
In 2003, NIST developed a new Certification & Accreditation (C&A) guideline known as FIPS 199. What levels of potential impact are defined by FIPS 199? Each correct answer represents a complete solution. Choose all that apply.
A. Moderate
B. Medium
C. High
D. Low
Answer: (SHOW ANSWER)
In 2003, NIST developed a new Certification & Accreditation (C&A) guideline known as FIPS 199. FIPS 199 is a standard for security categorization of Federal Information and Information Systems. It defines three levels of potential impact: Low: It causes a limited adverse effect. Medium: It causes a serious adverse effect. High: It causes a severe adverse effect.

NEW QUESTION: 127
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: 128
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: 129
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)
Explanation/Reference:
Explanation: 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. AnswerA is incorrect. It is a function performed by the ASSET system.

NEW QUESTION: 130
Which of the following US Acts emphasized a "risk-based policy for cost-effective security" and makes mandatory for agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget?
A. Federal Information Security Management Act of 2002 (FISMA)
B. The Electronic Communications Privacy Act of 1986 (ECPA)
C. The Equal Credit Opportunity Act (ECOA)

D. The Fair Credit Reporting Act (FCRA)

Answer: A (LEAVE A REPLY)

The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. 3541, et seq.) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899). The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA has brought attention within the federal government to cybersecurity and explicitly emphasized a "risk-based policy for cost-effective security". FISMA requires agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget (OMB). OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act. Answer C is incorrect. The Equal Credit Opportunity Act (ECOA) is a United States law (codified at 15 U.S.C. 1691 et seq.), enacted in 1974, that makes it unlawful for any creditor to discriminate against any applicant, with respect to any aspect of a credit transaction, on the basis of race, color, religion, national origin, sex, marital status, or age; to the fact that all or part of the applicant's income derives from a public assistance program; or to the fact that the applicant has in good faith exercised any right under the Consumer Credit Protection Act. The law applies to any person who, in the ordinary course of business, regularly participates in a credit decision, including banks, retailers, bankcard companies, finance companies, and credit unions. Answer B is incorrect. The Electronic Communications Privacy Act of 1986 (ECPA Pub.L. 99-508, Oct. 21, 1986, 100 Stat. 1848, 18 U.S.C. 2510) was enacted by the United States Congress to extend government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer. Specifically, ECPA was an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Wiretap Statute), which was primarily designed to prevent unauthorized government access to private electronic communications. The ECPA also added new provisions prohibiting access to stored electronic communications, i.e., the Stored Communications Act,18 U.S.C. 2701-2712. Answer D is incorrect. The Fair Credit Reporting Act (FCRA) is an American federal law (codified at 15 U.S.C. 1681 et seq.) that regulates the collection, dissemination, and use of consumer information, including consumer credit information. Along with the Fair Debt Collection Practices Act (FDCPA), it forms the base of consumer credit rights in the United States. It was originally passed in 1970, and is enforced by the US Federal Trade Commission.

NEW QUESTION: 131

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

A. Security operations

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

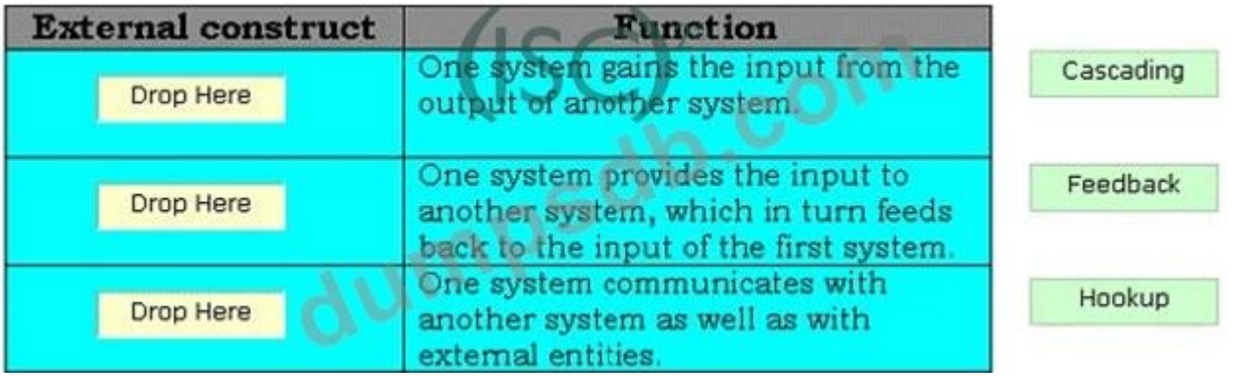
NEW QUESTION: 132
Which of the following methods is a means of ensuring that system changes are approved before being implemented, only the proposed and approved changes are implemented, and the implementation is complete and accurate?
A. Configuration control
B. Documentation control
C. Configuration identification
D. Configuration auditing
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: Documentation control is a method of ensuring that system changes should be agreed upon before being implemented, only the proposed and approved changes are implemented, and the implementation is complete and accurate. Documentation control is involved in the strict events for proposing, monitoring, and approving system changes and their implementation. It helps the change process by supporting the person who synchronizes the analytical task, approves system changes, reviews the implementation of changes, and oversees other tasks such as documenting the controls.
AnswerD 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. 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. Answer C 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.

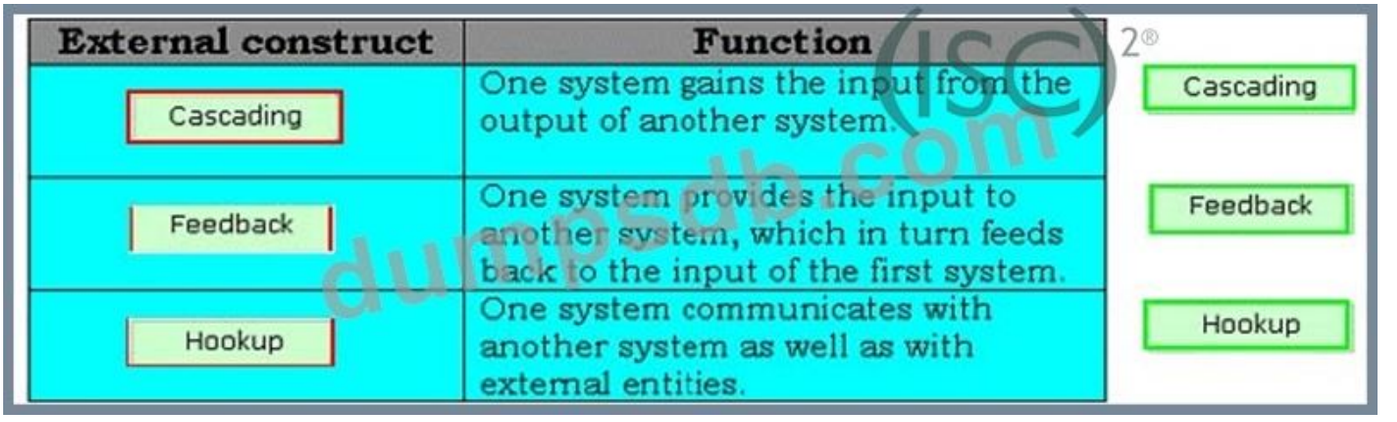
NEW QUESTION: 133

DRAG DROP

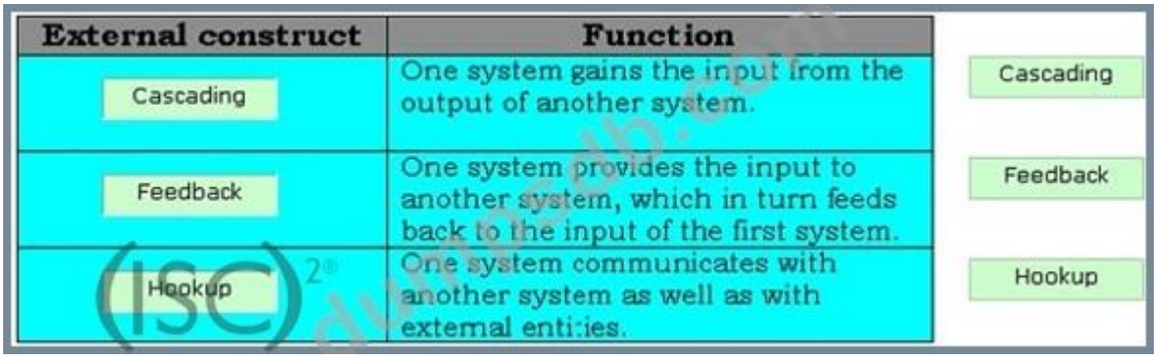
Drag and drop the appropriate external constructs in front of their respective functions.



Answer:



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: 134
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: (SHOW ANSWER)
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: 135
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: 136
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: 137
A part of a project deals with the hardware work. As a project manager, you have decided to hire a company to deal with all hardware work on the project. Which type of risk response is this?
A. Exploit
B. Mitigation
C. Transference
D. Avoidance
Answer: (SHOW ANSWER)
When you are hiring a third party to own risk, it is known as transference risk response. 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. Answer B is incorrect. The act of spending money to reduce a risk probability and impact is known as mitigation. Answer A is incorrect. Exploit is a strategy that may be selected for risks with positive impacts where the organization wishes to ensure that the opportunity is realized. Answer D is incorrect. When extra activities are introduced into the project to avoid the risk, this is an example of avoidance.

NEW QUESTION: 138
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: 139

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: 140

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)

Explanation/Reference:

Explanation: 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. AnswerA 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 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: 141
Which of the following types of activities can be audited for security? Each correct answer represents a complete solution. Choose three.
A. File and object access
B. Data downloading from the Internet
C. Printer access
D. Network logons and logoffs
Answer: A,C,D (LEAVE A REPLY)
Explanation/Reference:
Explanation: The following types of activities can be audited: Network logons and logoffs File access Printer access Remote access service Application usage Network services 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 security auditing, the type of event to be audited should be specified in the audit policy. Auditing is an essential component to maintain the security of deployed systems. Security auditing depends on the criticality of the environment and on the company's security policy. The security system should be reviewed periodically. Answer: B is incorrect. Data downloading from the Internet cannot be audited.

NEW QUESTION: 142
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: (SHOW ANSWER)
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: 143
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: 144
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: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: 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. AnswerD 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.
AnswerA 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.
AnswerB 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: 145
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: C (LEAVE A REPLY)
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: 146
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: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: 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

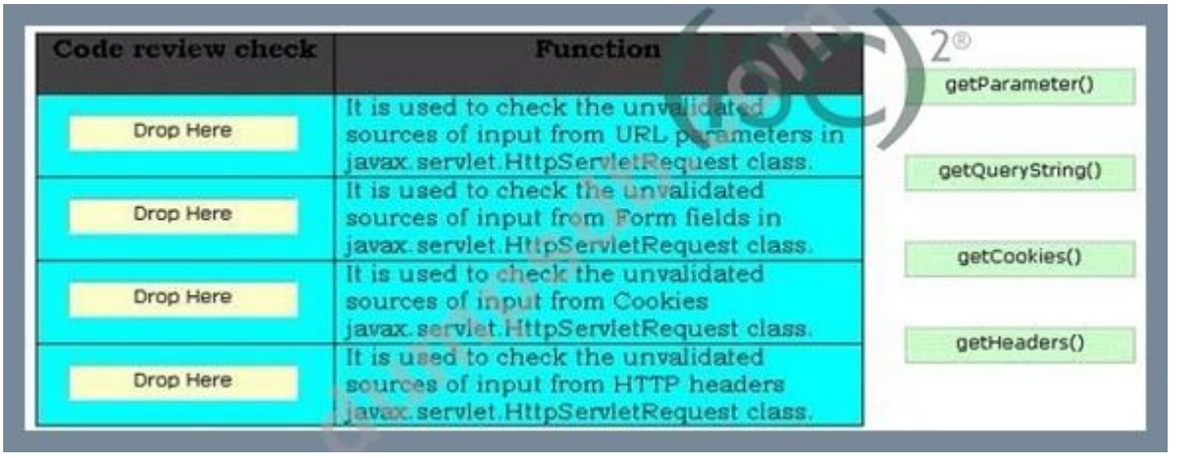
within a known environment through the security accreditation phase. In many organizations, the authorizing official is also referred as approving/accrediting authority (DAA) or the Principal Approving Authority (PAA). AnswerC is incorrect. The system owner has the responsibility of informing the key 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. AnswerD is incorrect. The CISO has the responsibility of carrying out the CIO's FISMA responsibilities. He manages the information security program functions.

NEW QUESTION: 147
Adrian is the project manager of the NHP Project. In her project there are several work packages that deal with electrical wiring. Rather than to manage the risk internally she has decided to hire a vendor to complete all work packages that deal with the electrical wiring. By removing the risk internally to a licensed electrician Adrian feels more comfortable with project team being safe. What type of risk response has Adrian used in this example?
A. Acceptance
B. Avoidance
C. Mitigation
D. Transference
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: This is an example of transference. When the risk is transferred to a third party, usually for a fee, it creates a contractual-relationship for the third party to manage the risk on behalf of the performing organization. Risk response planning is a method of developing options to decrease the amount of threats and make the most of opportunities. The risk response should be aligned with the consequence of the risk and cost-effectiveness. This planning documents the processes for managing risk events. It addresses the owners and their responsibilities, risk identification, results from qualification and quantification processes, budgets and times for responses, and contingency plans. The various risk response planning techniques are as follows: Risk acceptance: It indicates that the project team has decided not to change the project management plan to deal with a risk, or is unable to identify any other suitable response strategy. Risk avoidance: It is a technique for a threat, which creates changes to the project management plan that are meant to either eliminate the risk or to protect the project objectives from this impact. Risk mitigation: It is a list of specific actions being taken to deal with specific risks associated with the threats and seeks to reduce the probability of occurrence or impact of risk below an

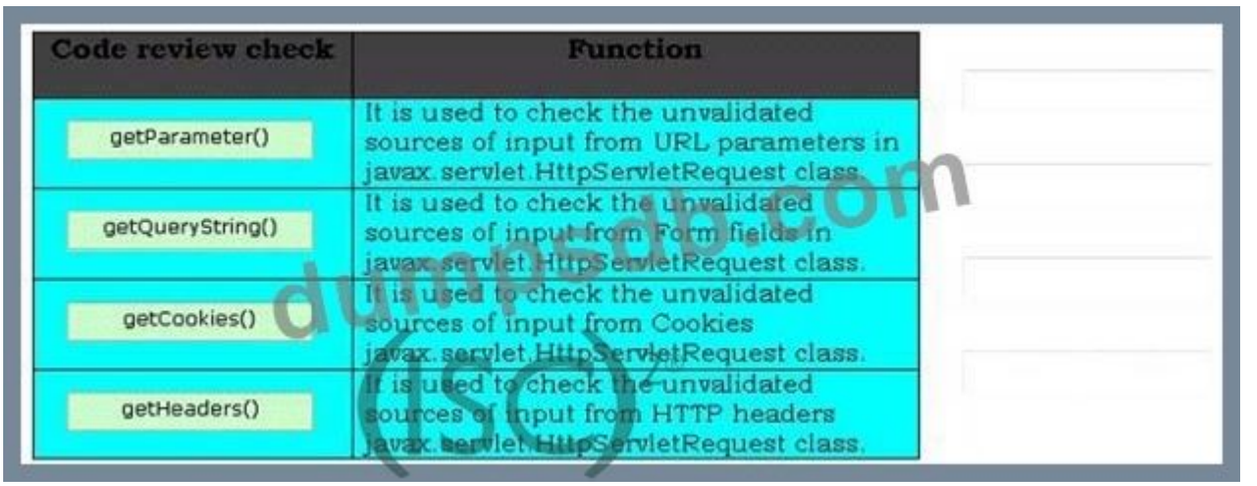
acceptable threshold. Risk transference: It is used to shift the impact of a threat to a third party, together with the ownership of the response.

NEW QUESTION: 148
Which of the following programming languages are compiled into machine code and directly executed by the CPU of a computer system? Each correct answer represents a complete solution. Choose two.
A. C
B. Microosft.NET
C. Java EE
D. C++
Answer: A,D (LEAVE A REPLY)
C and C++ programming languages are unmanaged code. Unmanaged code is compiled into machine code and directly executed by the CPU of a computer system. Answer C and B are incorrect. Java EE and Microsoft.Net are compiled into an intermediate code format.

NEW QUESTION: 149
DRAG DROP
Security code review identifies the unvalidated input calls made by an attacker and avoids those calls to be processed by the server. It performs various review checks on the stained calls of servlet for identifying unvalidated input from the attacker. Choose the appropriate review checks and drop them in front of their respective functions.
Select and Place:



Answer:



Explanation/Reference:

Explanation: The various security code review checks performed on the stained calls of servlet are as follows: getParameter(): It is used to check the unvalidated sources of input from URL parameters in javax.servlet.HttpServletRequest class. getQueryString(): It is used to check the unvalidated sources of input from Form fields in javax.servlet.HttpServletRequest class. getCookies(): It is used to check the unvalidated sources of input from Cookies javax.servlet.HttpServletRequest class. getHeaders(): It is used to check the unvalidated sources of input from HTTP headers javax.servlet.HttpServletRequest class.

NEW QUESTION: 150

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: 151

Which of the following are the types of intellectual property? Each correct answer represents a complete solution. Choose all that apply.

A. Patent

B. Copyright

C. Standard

D. Trademark

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

Common types of intellectual property include copyrights, trademarks, patents, industrial design rights, and trade secrets. 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. A trademark is a distinctive sign used by an individual, business organization, or other legal entity to identify that the products or services to consumers with which the trademark appears originate from a unique source, and to distinguish its products or services from those of other entities. A trademark is designated by the following symbols: : It is for an unregistered trade mark and it is used to promote or brand goods. : It is for an unregistered service mark and it is used to promote or brand services. : It is for a registered trademark. A patent is a set of exclusive rights granted by a state to an inventor or their assignee for a limited period of time in exchange for a public disclosure of an invention. Answer C is incorrect. It is not a type of intellectual property.

NEW QUESTION: 152

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: 153
You work as a Security Manager for Tech Perfect Inc. You have set up a SIEM server for the following purposes: Analyze the data from different log sources Correlate the events among the log entries Identify and prioritize significant events Initiate responses to events if required One of your log monitoring staff wants to know the features of SIEM product that will help them in these purposes. What features will you recommend? Each correct answer represents a complete solution. Choose all that apply.
A. Asset information storage and correlation
B. Transmission confidentiality protection
C. Incident tracking and reporting
D. Security knowledge base
E. Graphical user interface
Answer: A,C,D,E (LEAVE A REPLY)

The features of SIEM products are as follows: Graphical user interface (GUI): It is used in analysis for identifying potential problems and reviewing all available data that are associated with the problems. Security knowledge base: It includes information on known vulnerabilities, log messages, and other technical data. Incident tracking and hacking: It has robust workflow features to track and report incidents. Asset information storage and correlation: It gives higher priority to an attack that affects a vulnerable OS or a main host. Answer B is incorrect. SIEM product does not have this feature.

NEW QUESTION: 154
Which of the following penetration testing techniques automatically tests every phone line in an exchange and tries to locate modems that are attached to the network?
A. Demon dialing
B. Sniffing
C. Social engineering
D. Dumpster diving
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation: The demon dialing technique automatically tests every phone line in an exchange and tries to locate modems that are attached to the network. Information about these modems can then be used to attempt external unauthorized access. Answer: B is incorrect. In sniffing, a protocol analyzer is used to capture data packets that are later decoded to collect information such as passwords or infrastructure configurations. Answer: D is incorrect. Dumpster diving technique is used for searching paper disposal areas for unshredded or otherwise improperly disposed-of reports. Answer: C is incorrect. Social engineering is the most commonly used technique of all, getting information (like passwords) just by asking for them.