

ISC.CSSLP.v2022-12-31.q209

Exam Code:	CSSLP
Exam Name:	Certified Secure Software Lifecycle Professional Practice Test
Certification Provider:	ISC
Free Question Number:	209
Version:	v2022-12-31
# of views:	1957
# of Questions views:	9418
https://www.dumpsfiles.com/files/ISC/CSSLP/ISC.CSSLP.v2022-12-31.q209	

NEW QUESTION: 1

Shoulder surfing is a type of in-person attack in which the attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard of an employee's computer while he is typing in his password at any access point such as a terminal/Web site. Which of the following is violated in a shoulder surfing attack?

- A. Integrity
- B. Availability
- C. Confidentiality
- D. Authenticity

Answer: C (LEAVE A REPLY)

Confidentiality is violated in a shoulder surfing attack. The CIA triad provides the following three tenets for which security practices are measured: Confidentiality: It is the property of preventing disclosure of information to unauthorized individuals or systems. Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Integrity: It means that data cannot be modified without authorization. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on. Availability: It means that data must be available at every time when it is needed. Answer D is incorrect. Authenticity is not a tenet of the CIA triad.

NEW QUESTION: 2

You work as a CSO (Chief Security Officer) for Tech Perfect Inc. You want to perform the following tasks: Develop a risk-driven enterprise information security architecture. Deliver security

infrastructure solutions that support critical business initiatives. Which of the following methods will you use to accomplish these tasks?

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

Answer: C ([LEAVE A REPLY](#))

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

NEW QUESTION: 3

Which of the following are Service Level Agreement (SLA) structures as defined by ITIL? Each correct answer represents a complete solution. Choose all that apply.

- A. Component Based
- B. Service Based
- C. Segment Based
- D. Customer Based
- E. Multi-Level

Answer: B,D,E ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: ITIL defines 3 types of Service Level Agreement (SLA) structures, which are as follows:

1.Customer Based: It covers all services used by an individual customer group. 2.Service Based: It is one service for all customers. 3.Multi-Level: Some examples of Multi-Level SLA are 3 Tier SLA encompassing Corporate and Customer & Service Layers. Answer C and A are incorrect. There are no such SLA structures as Segment Based and Component Based.

NEW QUESTION: 4

Which of the following acts is used to recognize the importance of information security to the economic and national security interests of the United States?

- A. Computer Misuse Act
- B. Lanham Act
- C. Computer Fraud and Abuse Act
- D. FISMA

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: The Federal Information Security Management Act of 2002 is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002. The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA has brought attention within the federal government to cybersecurity and explicitly emphasized a 'risk-based policy for cost-effective security'. FISMA requires agency program officials, chief information officers, and Inspectors 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:

B is incorrect. The Lanham Act is a piece of legislation that contains the federal statutes of trademark law in the United States. The Act prohibits a number of activities, including trademark infringement, trademark dilution, and false advertising. It is also called Lanham Trademark Act. Answer A is incorrect. The Computer Misuse Act 1990 is an act of the UK Parliament which states the following statement:

Unauthorized access to the computer material is punishable by 6 months imprisonment or a fine "not exceeding level 5 on the standard scale" (currently 5000). Unauthorized access with the intent to commit or facilitate commission of further offences is punishable by 6 months/maximum fine on summary conviction or 5 years/fine on indictment. Unauthorized modification of computer material is subject to the same sentences as section 2 offences.

Answer C is incorrect. The Computer Fraud and Abuse Act is a law passed by the United States Congress in 1984 intended to reduce cracking of computer systems and to address federal computer-related offenses. The Computer Fraud and Abuse Act (codified as 18 U.S.C. 1030) governs cases with a compelling federal interest, where computers of the federal government or certain financial institutions are involved, where the crime itself is interstate in nature, or computers used in interstate and foreign commerce. It was amended in 1986, 1994, 1996, in 2001 by the USA PATRIOT Act, and in 2008 by the Identity Theft Enforcement and Restitution Act. Section (b) of the act punishes anyone who not just commits or attempts to commit an offense under the Computer Fraud and Abuse Act but also those who conspire to do so.

NEW QUESTION: 5

Which of the following governance bodies provides management, operational and technical controls to satisfy security requirements?

- A. Senior Management
- B. Business Unit Manager
- C. Information Security Steering Committee
- D. Chief Information Security Officer

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Explanation: Senior management provides management, operational and technical controls to satisfy security requirements. The governance roles and responsibilities are mentioned below in the table:

Governance Body	Membership	Responsibilities
Information Security Steering Committee	CFO, CEO, COO, CTO, VP Business units chaired by CISO	It establishes and supports security programs.
Senior Management	C-level, unit VPs and senior VPs	It provides management, operational and technical controls to satisfy security requirements.
Chief Information Security Officer	CISO and staff	It directs and coordinates implementations of information security program.
Business Unit Managers	Department heads and supervisors	They classify and establish requirements for safeguarding information assets.

NEW QUESTION: 6

According to the NIST SAMATE, dynamic analysis tools operate by generating runtime vulnerability scenario using some functions. Which of the following are functions that are used by the dynamic analysis tools and are summarized in the NIST SAMATE? Each correct answer represents a complete solution. Choose all that apply.

- A. Implementation attack
- B. Source code security
- C. File corruption
- D. Network fault injection

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

According to the NIST SAMATE, dynamic analysis tools operate by generating runtime vulnerability scenario using the following functions: Resource fault injection Network fault injection System fault injection User interface fault injection Design attack Implementation attack File corruption Answer B is incorrect. This function is summarized for static analysis tools.

NEW QUESTION: 7

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. Answer D is incorrect. Virtualization increases configuration effort because of complexity of the virtualization layer and composite system.

NEW QUESTION: 8

Which of the following tiers addresses risks from an information system perspective?

- A. Tier 0
- B. Tier 3
- C. Tier 2
- D. Tier 1

Answer: [B \(LEAVE A REPLY\)](#)

Explanation/Reference:

Explanation: The information system level is the tier 3. It addresses risks from an information system perspective, and is guided by the risk decisions at tiers 1 and 2. Risk decisions at tiers 1 and 2 impact the ultimate selection and deployment of requisite safeguards. This also has an impact on the countermeasures at the information system level. The RMF primarily operates at tier 3 but it can also have interactions at tiers 1 and 2. Answer A is incorrect. It is an invalid Tier description. Answer: D is incorrect.

The Organization Level is the Tier 1, and it addresses risks from an organizational perspective. Answer C is incorrect. The mission and business process level is the Tier 2, and it addresses risks from the mission and business process perspective.

NEW QUESTION: 9

In which of the following cryptographic attacking techniques does an attacker obtain encrypted messages that have been encrypted using the same encryption algorithm?

- A. Chosen plaintext attack
- B. Chosen ciphertext attack
- C. Ciphertext only attack
- D. Known plaintext attack

Answer: [C \(LEAVE A REPLY\)](#)

In a ciphertext only attack, an attacker obtains encrypted messages that have been encrypted using the same encryption algorithm.

NEW QUESTION: 10

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: 11

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

- A. DoD 8910.1
- B. DoD 5200.22-M
- C. DoD 8000.1
- D. DoD 5200.40

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: DITSCAP stands for DoD Information Technology Security Certification and Accreditation Process. The DoD Directive 5200.40 (DoD Information Technology Security Certification and Accreditation Process) established the DITSCAP as the standard C&A process for the Department of Defense. The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of

Defense (DoD) for managing risk. DIACAP replaced the former process, known as DITSCAP, in 2006. AnswerB is incorrect. This DoD Directive is known as National Industrial Security Program Operating Manual. AnswerC is incorrect. This DoD Directive is known as Defense Information Management (IM) Program. AnswerA is incorrect. This DoD Directive is known as Management and Control of Information Requirements.

NEW QUESTION: 12

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: 13

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)

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: 14

Who amongst the following makes the final accreditation decision?

- A. ISSE
- B. CRO
- C. DAA
- D. ISSO

Answer: C (LEAVE A REPLY)

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. Answer D is incorrect. An Information System Security Officer (ISSO) plays the role of a supporter. The responsibilities of an Information System Security Officer (ISSO) are as follows: Manages the security of the information system that is slated for Certification & Accreditation (C&A). Insures the information systems configuration with the agency's information security policy. Supports the information system owner/information owner for the completion of security-related responsibilities. Takes part in the formal configuration management process. Prepares Certification & Accreditation (C&A) packages. Answer A 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. Answer B is incorrect. A Chief Risk Officer (CRO) is also known as Chief Risk Management Officer (CRMO). The Chief Risk Officer or Chief Risk Management Officer of a corporation is the executive accountable for enabling the efficient and effective governance of significant risks, and related opportunities, to a business and its various segments. Risks are commonly categorized as strategic, reputational, operational, financial, or compliance-related. CRO's are accountable to the Executive Committee and The Board for enabling the business to balance risk and reward. In more complex organizations, they are generally responsible for coordinating the organization's Enterprise Risk Management (ERM) approach.

NEW QUESTION: 15

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: 16

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: ([SHOW ANSWER](#))

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 onetime 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).

Valid CSSLP Dumps shared by TrainingDump.com for Helping Passing CSSLP Exam! TrainingDump.com now offer the **newest CSSLP exam dumps**, the TrainingDump.com CSSLP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CSSLP dumps with Test Engine here:
<https://www.trainingdump.com/ISC/CSSLP-practice-exam-dumps.html> (349 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 17

Which of the following are the levels of public or commercial data classification system? Each correct answer represents a complete solution. Choose all that apply.

- A. Sensitive
- B. Private
- C. Unclassified
- D. Confidential
- E. Secret
- F. Public

Answer: ([SHOW ANSWER](#))

The public or commercial data classification is also built upon a four-level model, which are as follows: Public Sensitive Private Confidential Each level (top to bottom) represents an increasing level of sensitivity. The public level is similar to unclassified level military classification system. This level of data should not cause any damage if disclosed. Sensitive is a higher level of classification than public level data. This level of data requires a greater level of protection to maintain confidentiality. The Private level of data is intended for company use only. Disclosure of this level of data can damage the company. The Confidential level of data is considered very sensitive and is intended for internal use only. Disclosure of this level of data can cause serious damage to the company. Answer C and E are incorrect. Unclassified and secret are the levels of military data classification.

NEW QUESTION: 18

The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum standard process for the certification and accreditation of computer and telecommunications systems that handle U.S. national security information. What are the different types of NIACAP accreditation? Each correct answer represents a complete solution. Choose all that apply.

- A. Site accreditation
- B. Type accreditation
- C. Secure accreditation
- D. System accreditation

Answer: A,B,D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: NIACAP accreditation is of three types depending on what is being certified. They are as follows: 1.Site accreditation: This type of accreditation evaluates the applications and systems at a specific, self contained location. 2.Type accreditation: This type of accreditation evaluates an application or system that is distributed to a number of different locations. 3.System accreditation: This accreditation evaluates a major application or general support system.

AnswerC is incorrect. No such type of NIACAP accreditation exists.

NEW QUESTION: 19

Which of the following testing methods verifies the interfaces between components against a software design?

- A. Regression testing
- B. Integration testing
- C. Black-box testing
- D. Unit testing

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: Integration testing is a software testing that seeks to verify the interfaces between components against a software design. Software components may be integrated in an iterative

way or all together ("big bang"). Normally the former is considered a better practice since it allows interface issues to be localized more quickly and fixed. Integration testing works to expose defects in the interfaces and interaction between the integrated components (modules).

Progressively larger groups of tested software components corresponding to elements of the architectural design are integrated and tested until the software works as a system. Answer: A is incorrect. Regression testing focuses on finding defects after a major code change has occurred. Specifically, it seeks to uncover software regressions, or old bugs that have come back. Such regressions occur whenever software functionality that was previously working correctly stops working as intended. Typically, regressions occur as an unintended consequence of program changes, when the newly developed part of the software collides with the previously existing code. Answer: D is incorrect. Unit testing refers to tests that verify the functionality of a specific section of code, usually at the function level. In an object-oriented environment, this is usually at the class level, and the minimal unit tests include the constructors and destructors. These types of tests are usually written by developers as they work on code (white-box style), to ensure that the specific function is working as expected. One function might have multiple tests, to catch corner cases or other branches in the code. Unit testing alone cannot verify the functionality of a piece of software, but rather is used to assure that the building blocks the software uses work independently of each other. Answer: C is incorrect. The black-box testing uses external descriptions of the software, including specifications, requirements, and design to derive test cases. These tests can be functional or non-functional, though usually functional. The test designer selects valid and invalid inputs and determines the correct output. There is no knowledge of the test object's internal structure. This method of test design is applicable to all levels of software testing: unit, integration, functional testing, system and acceptance. The higher the level, and hence the bigger and more complex the box, the more one is forced to use black box testing to simplify. While this method can uncover unimplemented parts of the specification, one cannot be sure that all existent paths are tested.

NEW QUESTION: 20

To help review or design security controls, they can be classified by several criteria. One of these criteria is based on time. According to this criteria, which of the following controls are intended to prevent an incident from occurring?

- A. Corrective controls
- B. Adaptive controls
- C. Detective controls
- D. Preventive controls

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: Preventive controls are the security controls that are intended to prevent an incident from occurring, e.g., by locking out unauthorized intruders. Answer C is incorrect. Detective controls are intended to identify and characterize an incident in progress, e.g., by sounding the intruder alarm and alerting the security guards or police. Answer A is incorrect. Corrective

controls are intended to limit the extent of any damage caused by the incident, e.g., by recovering the organization to normal working status as efficiently as possible. Answer: B is incorrect. There is no such categorization of controls based on time.

NEW QUESTION: 21

What are the subordinate tasks of the Initiate and Plan IA C&A phase of the DIACAP process? Each correct answer represents a complete solution. Choose all that apply.

- A. Initiate IA implementation plan
- B. Develop DIACAP strategy
- C. Assign IA controls.
- D. Assemble DIACAP team
- E. Register system with DoD Component IA Program.
- F. Conduct validation activity.

Answer: ([SHOW ANSWER](#))

The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk. The subordinate tasks of the Initiate and Plan IA C&A phase are as follows: Register system with DoD Component IA Program. Assign IA controls. Assemble DIACAP team. Develop DIACAP strategy. Initiate IA implementation plan. Answer F is incorrect. Validation activities are conducted in the second phase of the DIACAP process, i.e., Implement and Validate Assigned IA Controls.

NEW QUESTION: 22

Which of the following elements of the BCP process emphasizes on creating the scope and the additional elements required to define the parameters of the plan?

- A. Business continuity plan development
- B. Plan approval and implementation
- C. Business impact analysis
- D. Scope and plan initiation

Answer: D ([LEAVE A REPLY](#))

The scope and plan initiation process in BCP symbolizes the beginning of the BCP process. It emphasizes on creating the scope and the additional elements required to define the parameters of the plan. The scope and plan initiation phase embodies a check of the company's operations and support services. The scope activities include creating a detailed account of the work required, listing the resources to be used, and defining the management practices to be employed. Answer C is incorrect. The business impact assessment is a method used to facilitate business units to understand the impact of a disruptive event. This phase includes the execution of a vulnerability assessment. This process makes out the mission-critical areas and business processes that are important for the survival of business. It is similar to the risk assessment process. The function of a business impact assessment process is to create a document, which is used to help and understand what impact a disruptive event would have on the business. Answer A is incorrect. The business continuity plan development refers to the utilization of the information

collected in the Business Impact Analysis (BIA) for the creation of the recovery strategy plan to support the critical business functions. The information gathered from the BIA is mapped out to make a strategy for creating a continuity plan. The business continuity plan development process includes the areas of plan implementation, plan testing, and ongoing plan maintenance. This phase also consists of defining and documenting the continuity strategy. Answer B is incorrect. The plan approval and implementation process involves creating enterprise-wide awareness of the plan, getting the final senior management signoff, and implementing a maintenance procedure for updating the plan as required.

NEW QUESTION: 23

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: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: 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. AnswerC is incorrect. It is not a type of intellectual property.

NEW QUESTION: 24

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](#))

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: 25

Which of the following terms ensures that no intentional or unintentional unauthorized modification is made to data?

- A. Non-repudiation
- B. Integrity
- C. Authentication
- D. Confidentiality

Answer: ([SHOW ANSWER](#)**)**

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: 26

An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

- A. Backup policy
- B. User password policy
- C. Privacy policy
- D. Network security policy

Answer: ([SHOW ANSWER](#)**)**

Monitoring the computer hard disks or e-mails of employees pertains to the privacy policy of an organization. Answer A is incorrect. The backup policy of a company is related to the backup of its data. Answer D is incorrect. The network security policy is related to the security of a company's network. Answer B is incorrect. The user password policy is related to passwords that users provide to log on to the network.

NEW QUESTION: 27

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: 28

You are advising a school district on disaster recovery plans. In case a disaster affects the main IT centers for the district they will need to be able to work from an alternate location. However, budget is an issue. Which of the following is most appropriate for this client?

- A. Cold site
- B. Off site
- C. Warm site
- D. Hot site

Answer: A ([LEAVE A REPLY](#))

A cold site provides an office space, and in some cases basic equipment. However, you will need to restore your data to that equipment in order to use it. This is a much less expensive solution than the hot site. Answer D is incorrect. A hot site has equipment installed, configured and ready to use. This may make disaster recovery much faster, but will also be more expensive. And a school district can afford to be down for several hours before resuming IT operations, so the less expensive option is more appropriate. Answer C is incorrect. A warm site is between a hot and cold site. It has some equipment ready and connectivity ready. However, it is still significantly more expensive than a cold site, and not necessary for this scenario. Answer B is incorrect. Off site is not any type of backup site terminology.

NEW QUESTION: 29

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](#))

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. Answer B 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: 30

Mark is the project manager of the NHQ project in StarTech Inc. The project has an asset valued at \$195,000 and is subjected to an exposure factor of 35 percent. What will be the Single Loss Expectancy of the project?

- A. \$68,250
- B. \$92,600
- C. \$72,650
- D. \$67,250

Answer: A ([LEAVE A REPLY](#))

The Single Loss Expectancy (SLE) of this project will be \$68,250. Single Loss Expectancy is a term related to Risk Management and Risk Assessment. It can be defined as the monetary value expected from the occurrence of a risk on an asset. It is mathematically expressed as follows: Single Loss Expectancy (SLE) = Asset Value (AV) * Exposure Factor (EF) where the Exposure Factor is represented in the impact of the risk over the asset, or percentage of asset lost. As an example, if the Asset Value is reduced two thirds, the exposure factor value is .66. If the asset is completely lost, the Exposure Factor is 1.0. The result is a monetary value in the same unit as the Single Loss Expectancy is expressed. Here, it is as follows: $SLE = Asset\ Value * Exposure\ Factor = 195,000 * 0.35 = \$68,250$ Answer B, C, and D are incorrect. These are not valid SLE's for this project.

NEW QUESTION: 31

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

- A. Contingency plan
- B. Business continuity plan
- C. Crisis communication plan
- D. Disaster recovery plan

Answer: ([SHOW ANSWER](#)**)**

The business continuity plan is designed to protect critical business processes from natural or man-made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan. Answer C is incorrect. The crisis communication plan can be broadly defined as the plan for the exchange of information before, during, or after a crisis event. It is considered as a sub-specialty of the public relations profession that is designed to protect and defend an individual, company, or organization facing a public challenge to its reputation. The aim of crisis communication plan is to assist organizations to achieve continuity of critical business processes and information flows under crisis, disaster or

event driven circumstances. Answer A is incorrect. A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and "triggers" for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption. Answer D is incorrect. A disaster recovery plan should contain data, hardware, and software that can be critical for a business. It should also include the plan for sudden loss such as hard disc crash. The business should use backup and data recovery utilities to limit the loss of data.

Valid CSSLP Dumps shared by TrainingDump.com for Helping Passing CSSLP Exam! TrainingDump.com now offer the **newest CSSLP exam dumps**, the TrainingDump.com CSSLP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CSSLP dumps with Test Engine here:
<https://www.trainingdump.com/ISC/CSSLP-practice-exam-dumps.html> (349 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 32

Henry is the project manager of the QBG Project for his company. This project has a budget of \$4,576,900 and is expected to last 18 months to complete. The CIO, a stakeholder in the project, has introduced a scope change request for additional deliverables as part of the project work. What component of the change control system would review the proposed changes' impact on the features and functions of the project's product?

- A.** Configuration management system
- B.** Scope change control system
- C.** Cost change control system
- D.** Integrated change control

Answer: A ([LEAVE A REPLY](#))

The configuration management system ensures that proposed changes to the project's scope are reviewed and evaluated for their affect on the project's product. Configuration Management System is a subsystem of the overall project management system. It is a collection of formal documented procedures used to identify and document the functional and physical characteristics of a product, result, service, or component of the project. It also controls any changes to such characteristics, and records and reports each change and its implementation status. It includes the documentation, tracking systems, and defined approval levels necessary for authorizing and controlling changes. Audits are performed as part of configuration management to determine if the requirements have been met. Answer B is incorrect. The scope change control system

focuses on reviewing the actual changes to the project scope. When a change to the project's scope is proposed, the configuration management system is also invoked. Answer C is incorrect. The cost change control system is responsible for reviewing and controlling changes to the project costs. Answer D is incorrect. Integrated change control examines the affect of a proposed change on the project as a whole.

NEW QUESTION: 33

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](#))

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: 34

The rights of an author or a corporation to make profit from the creation of their products (such as software, music, etc.) are protected by the Intellectual Property law. Which of the following are the components of the Intellectual Property law? Each correct answer represents a part of the solution. Choose two.

- A. Trademark law
- B. Industrial Property law
- C. Copyright law
- D. Patent law

Answer: B,C ([LEAVE A REPLY](#))

Explanation/Reference:

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

NEW QUESTION: 35

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](#))

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: 36

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: 37

Which of the following governance bodies directs and coordinates implementations of the information security program?

- A. Chief Information Security Officer
- B. Information Security Steering Committee
- C. Business Unit Manager
- D. Senior Management

Answer: A ([LEAVE A REPLY](#))

Chief Information Security Officer directs and coordinates implementations of the information security program. The governance roles and responsibilities are mentioned below in the table:

NEW QUESTION: 38

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

- A. Copyright
- B. Snooping
- C. Utility model
- D. Patent

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: A patent is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention. Answer: A is incorrect. A copyright is a form of intellectual property, which secures to its holder the exclusive right to produce copies of his or her works of original expression, such as a literary work, movie, musical work or sound recording, painting, photograph, computer program, or industrial design, for a

defined, yet extendable, period of time. It does not cover ideas or facts. Copyright laws protect intellectual property from misuse by other individuals.

Answer B is incorrect. Snooping is an activity of observing the content that appears on a computer monitor

or watching what a user is typing. Snooping also occurs by using software programs to remotely monitor activity on a computer or network device. Hackers or attackers use snooping techniques and equipment such as keyloggers to monitor keystrokes, capture passwords and login information, and to intercept e-mail and other private communications. Sometimes, organizations also snoop their employees legitimately to monitor their use of organizations' computers and track Internet usage. Answer: C is incorrect. A utility model is an intellectual property right to protect inventions.

NEW QUESTION: 39

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

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

Answer: (SHOW ANSWER)

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

NEW QUESTION: 40

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

- A.** Developing an organization-wide information protection strategy and incorporating high-level information security requirements
- B.** Defining the types of information that the organization needs, to successfully execute the stated missions and business processes
- C.** Specifying the degree of autonomy for the subordinate organizations
- D.** Defining the core missions and business processes for the organization
- E.** Prioritizing missions and business processes with respect to the goals and objectives of the organization

Answer: (SHOW ANSWER)

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: 41

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

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

Answer: D (LEAVE A REPLY)

Explanation/Reference:

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

NEW QUESTION: 42

Which of the following security architectures defines how to integrate widely disparate applications for a world that is Web-based and uses multiple implementation platforms?

- A. Sherwood Applied Business Security Architecture
- B. Enterprise architecture
- C. Service-oriented architecture
- D. Service-oriented modeling and architecture
- E. Explanation:

In computing, a service-oriented architecture (SOA) is a flexible set of design principles used during the phases of systems development and integration. A deployed SOA-based architecture will provide a loosely-integrated suite of services that can be used within multiple business domains. SOA also generally provides a way for consumers of services, such as web-based applications, to be aware of available SOA-based services. For example, several disparate departments within a company may develop and deploy SOA services in different implementation languages; their respective clients will benefit from a well understood, well defined interface to access them. XML is commonly used for interfacing with SOA services, though this is not required. SOA defines how to integrate widely disparate applications for a world that is Web-based and uses multiple implementation platforms. Rather than defining an API, SOA defines the interface in terms of protocols and functionality. An endpoint is the entry point for such an SOA implementation.

(Layer interaction in Service-oriented architecture)

Answer: (SHOW ANSWER)

is incorrect. SABSA (Sherwood Applied Business Security Architecture) is a framework and methodology for Enterprise Security Architecture and Service Management. SABSA is a model and a methodology for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives. The primary characteristic of the SABSA model is that everything must be derived from an analysis of the business requirements for security, especially those in which security has an enabling function through which new business opportunities can be developed and exploited. Answer D is incorrect. The service-oriented modeling and architecture (SOMA) includes an analysis and design method that extends traditional object-oriented and component-based analysis and design methods to include concerns relevant to and supporting SOA. Answer B is incorrect. Enterprise architecture describes the terminology, the composition of subsystems, and their relationships with the external environment, and the guiding principles for the design and evolution of an enterprise.

NEW QUESTION: 43

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: 44

Martha works as a Project Leader for BlueWell Inc. She and her team have developed accounting software. The software was performing well. Recently, the software has been modified. The users of this software are now complaining about the software not working properly. Which of the following actions will she take to test the software?

- A. Perform integration testing
- B. Perform regression testing
- C. Perform unit testing
- D. Perform acceptance testing

Answer: (SHOW ANSWER)

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.

Answer D is incorrect. The acceptance testing is performed on the application before its implementation into the production environment. It is done either by a client or an application specialist to ensure that the software meets the requirement for which it was made. Answer A is incorrect. Integration testing is a logical extension of unit testing. It is performed to identify the problems that occur when two or more units are combined into a component. During integration testing, a developer combines two units that have already been tested into a component, and tests the interface between the two units. Although integration testing can be performed in various ways, the following three approaches are generally used: The top-down approach The bottom-up approach The umbrella approach Answer C is incorrect. Unit testing is a type of testing in which each independent unit of an application is tested separately. During unit testing, a developer takes the smallest unit of an application, isolates it from the rest of the application code, and tests it to determine whether it works as expected. Unit testing is performed before integrating these independent units into modules. The most common approach to unit testing requires drivers and stubs to be written. Drivers and stubs are programs. A driver simulates a calling unit, and a stub simulates a called unit.

NEW QUESTION: 45

In which of the following DIACAP phases is residual risk analyzed?

- A. Phase 1
- B. Phase 5
- C. Phase 2
- D. Phase 4
- E. Phase 3

Answer: (SHOW ANSWER)

The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk. The Certification Determination and Accreditation phase is the third phase in the DIACAP process. Its subordinate tasks are as follows: Analyze residual risk. Issue certification

determination. Make accreditation decision. Answer A is incorrect. Phase 1 is known as Initiate and Plan IA C&A. Answer C is incorrect. Phase 2 is used to implement and validate assigned IA controls. Answer E is incorrect. Phase 3 is used to make certification determination and accreditation decisions. Answer B is incorrect. Phase 5 is known as decommission system and is used to conduct activities related to the disposition of the system data and objects.

NEW QUESTION: 46

DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. What phases are identified by DIACAP? Each correct answer represents a complete solution. Choose all that apply.

- A.** System Definition
- B.** Validation
- C.** Identification
- D.** Accreditation
- E.** Verification
- F.** Re-Accreditation

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

Explanation/Reference:

Explanation: The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk.

DIACAP replaced the former process, known as DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process), in 2006. DoD Instruction (DoDI) 8510.01 establishes a standard DoD-wide process with a set of activities, general tasks, and a management structure to certify and accredit an Automated Information System (AIS) that will maintain the Information Assurance (IA) posture of the Defense Information Infrastructure (DII) throughout the system's life cycle.

DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. It identifies four phases: 1.System Definition 2.Verification 3.Validation 4.Re-Accreditation

Valid CSSLP Dumps shared by TrainingDump.com for Helping Passing CSSLP Exam! TrainingDump.com now offer the **newest CSSLP exam dumps**, the TrainingDump.com CSSLP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CSSLP dumps with Test Engine here:

<https://www.trainingdump.com/ISC/CSSLP-practice-exam-dumps.html> (349 Q&As Dumps,

40%OFF Special Discount: Exam-Tests)

NEW QUESTION: 47

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: 48

Bill is the project manager of the JKH Project. He and the project team have identified a risk event in the project with a high probability of occurrence and the risk event has a high cost impact on the project. Bill discusses the risk event with Virginia, the primary project customer, and she decides that the requirements surrounding the risk event should be removed from the project. The removal of the requirements does affect the project scope, but it can release the project from the high risk exposure. What risk response has been enacted in this project?

- A. Mitigation
- B. Transference
- C. Acceptance
- D. Avoidance

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: This is an example of the avoidance risk response. Because the project plan has been changed to avoid the risk event, so it is considered the avoidance risk response. Risk avoidance is a technique used for threats. It creates changes to the project management plan that are meant to either eliminate the risk completely or to protect the project objectives from its impact. Risk avoidance removes the risk event entirely either by adding additional steps to avoid the event or reducing the project scope requirements. It may seem the answer to all possible risks, but avoiding risks also means losing out on the potential gains that accepting (retaining) the risk might have allowed. Answer: C is incorrect. Acceptance is when the stakeholders acknowledge the risk event and they accept that the event could happen and could have an impact on the project. Acceptance is usually used for risk events that have low risk exposure or risk events in which the project has no control, such as a pending law or weather threats. Answer: A is incorrect. Mitigation is involved with the actions to reduce an included risk's probability and/or impact on the project's objectives. As the risk was removed from the project, this scenario describes avoidance, not mitigation. Answer: B is incorrect. Transference is when the risk is still

within the project, but the ownership and management of the risk event is transferred to a third party - usually for a fee.

NEW QUESTION: 49

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. Which of the following statements are true about Certification and Accreditation? Each correct answer represents a complete solution. Choose two.

- A.** Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system.
- B.** Accreditation is a comprehensive assessment of the management, operational, and technical security controls in an information system.
- C.** Accreditation is the official management decision given by a senior agency official to authorize operation of an information system.
- D.** Certification is the official management decision given by a senior agency official to authorize operation of an information system.

Answer: A,C ([LEAVE A REPLY](#))

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.

NEW QUESTION: 50

Which of the following processes culminates in an agreement between key players that a system in its current configuration and operation provides adequate protection controls?

- A.** Information Assurance (IA)
- B.** Information systems security engineering (ISSE)
- C.** Certification and accreditation (C&A)
- D.** Risk Management

Answer: C ([LEAVE A REPLY](#))

Certification and accreditation (C&A) is a set of processes that culminate in an agreement between key players that a system in its current configuration and operation provides adequate protection controls. Certification and Accreditation (C&A or CnA) is a process for implementing

information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The C&A process is used extensively in the U.S. Federal Government. Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. Answer D is incorrect. Risk management is a set of processes that ensures a risk-based approach is used to determine adequate, cost-effective security for a system. Answer A is incorrect. Information assurance (IA) is the process of organizing and monitoring information-related risks. It ensures that only the approved users have access to the approved information at the approved time. IA practitioners seek to protect and defend information and information systems by ensuring confidentiality, integrity, authentication, availability, and non-repudiation. These objectives are applicable whether the information is in storage, processing, or transit, and whether threatened by an attack. Answer B is incorrect. ISSE is a set of processes and solutions used during all phases of a system's life cycle to meet the system's information protection needs.

NEW QUESTION: 51

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. Answer A 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: 52

Companies use some special marks to distinguish their products from those of other companies. These marks can include words, letters, numbers, drawings, etc. Which of the following terms describes these special marks?

- A. Business mark
- B. Trademark
- C. Sales mark
- D. Product mark

Answer: B ([LEAVE A REPLY](#))

A trademark is a mark that is used by a company to distinguish its products from those of other companies. There are various ways a company uses its trademark to distinguish its products from others. It can use words, letters, numbers, drawings, pictures, and so on, in its trademark. Answer D, A, and C are incorrect. There is no such mark as product mark, business mark, or sales mark.

NEW QUESTION: 53

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: 54

An asset with a value of \$600,000 is subject to a successful malicious attack threat twice a year. The asset has an exposure of 30 percent to the threat. What will be the annualized loss expectancy?

- A. \$360,000
- B. \$180,000

C. \$280,000

D. \$540,000

E. Explanation:

The annualized loss expectancy will be \$360,000. Annualized loss expectancy (ALE) is the annually expected financial loss to an organization from a threat. The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as follows:

$ALE = \text{Single Loss Expectancy (SLE)} * \text{Annualized Rate of Occurrence (ARO)}$

Here, it is as follows:

$SLE = \text{Asset value} * EF \text{ (Exposure factor)}$

$= 600,000 * (30/100)$

$= 600,000 * 0.30$

$= 180,000$

$ALE = SLE * ARO$

$= 180,000 * 2$

$= 360,000$

Answer: (SHOW ANSWER)

B, and D are incorrect. These are not valid answers.

NEW QUESTION: 55

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)

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: 56

What are the differences between managed and unmanaged code technologies? Each correct answer represents a complete solution. Choose two.

- A.** Managed code is referred to as Hex code, whereas unmanaged code is referred to as byte code.
- B.** C and C++ are the examples of managed code, whereas Java EE and Microsoft.NET are the examples of unmanaged code.
- C.** Managed code executes under management of a runtime environment, whereas unmanaged code is executed by the CPU of a computer system.
- D.** Managed code is compiled into an intermediate code format, whereas unmanaged code is compiled into machine code.

Answer: C,D ([LEAVE A REPLY](#))

Programming languages are categorized into two technologies: 1.Managed code: This computer program code is compiled into an intermediate code format. Managed code is referred to as byte code. It executes under the management of a runtime environment. Java EE and Microsoft.NET are the examples of managed code. 2.Unmanaged code: This computer code is compiled into machine code. Unmanaged code is executed by the CPU of a computer system. C and C++ are the examples of unmanaged code. Answer A is incorrect. Managed code is referred to as byte code. Answer B is incorrect. C and C++ are the examples of unmanaged code, whereas Java EE and Microsoft.NET are the examples of managed code.

NEW QUESTION: 57

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: 58

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](#))

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: 59

You are the project manager for GHY Project and are working to create a risk response for a negative risk.

You and the project team have identified the risk that the project may not complete on time, as required by the management, due to the creation of the user guide for the software you're creating. You have elected to hire an external writer in order to satisfy the requirements and to alleviate the risk event. What type of risk response have you elected to use in this instance?

- A. Transference
- B. Exploiting
- C. Avoidance
- D. Sharing

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: This is an example of transference as you have transferred the risk to a third party. Transference almost always is done with a negative risk event and it usually requires a contractual relationship.

NEW QUESTION: 60

Certification and Accreditation (C&A or CnA) is a process for implementing information security. Which of the following is the correct order of C&A phases in a DITSCAP assessment?

- A. Verification, Definition, Validation, and Post Accreditation
- B. Definition, Validation, Verification, and Post Accreditation
- C. Definition, Verification, Validation, and Post Accreditation
- D. Verification, Validation, Definition, and Post Accreditation

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: C&A consists of four phases in a DITSCAP assessment. These phases are the same as NIACAP phases. The order of these phases is as follows: 1. Definition: The definition phase is focused on understanding the IS business case, the mission, environment, and architecture. This phase determines the security requirements and level of effort necessary to achieve Certification & Accreditation (C&A).

2. Verification: The second phase confirms the evolving or modified system's compliance with the information. The verification phase ensures that the fully integrated system will be ready for certification testing. 3. Validation: The third phase confirms abidance of the fully integrated system with the security policy. This phase follows the requirements slated in the SSAA. The objective of the validation phase is to show the required evidence to support the DAA in accreditation process. 4. Post Accreditation: The Post Accreditation is the final phase of DITSCAP assessment and it starts after the system has been certified and accredited for operations. This phase ensures secure system management, operation, and maintenance to save an acceptable level of residual risk.

NEW QUESTION: 61

Stella works as a system engineer for BlueWell Inc. She wants to identify the performance thresholds of each build. Which of the following tests will help Stella to achieve her task?

- A. Reliability test
- B. Performance test
- C. Regression test
- D. Functional test

Answer: B ([LEAVE A REPLY](#))

The various types of internal tests performed on builds are as follows: Regression tests: It is also known as the verification testing. These tests are developed to confirm that capabilities in earlier builds continue to work correctly in the subsequent builds. Functional test: These tests emphasizes on verifying that the build meets its functional and data requirements and correctly generates each expected display and report. Performance tests: These tests are used to identify the performance thresholds of each build. Reliability tests: These tests are used to identify the reliability thresholds of each build.

Valid CSSLP Dumps shared by TrainingDump.com for Helping Passing CSSLP Exam! TrainingDump.com now offer the **newest CSSLP exam dumps**, the TrainingDump.com CSSLP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CSSLP dumps with Test Engine here:
<https://www.trainingdump.com/ISC/CSSLP-practice-exam-dumps.html> (349 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 62

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: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: 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: 63

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

- A. OMB
- B. NIST
- C. NSA/CSS
- D. DCAA

Answer: A ([LEAVE A REPLY](#))

The Office of Management and Budget (OMB) is a Cabinet-level office, and is the largest office within the Executive Office of the President (EOP) of the United States. The current OMB Director is Peter Orszag and was appointed by President Barack Obama. The OMB's predominant mission is to assist the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies. In helping to formulate the President's

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

NEW QUESTION: 64

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
- E.** 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.

Answer: D,E (LEAVE A REPLY)

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: 65

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: ([SHOW ANSWER](#))

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. Answer D 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: 66

Software Development Life Cycle (SDLC) is a logical process used by programmers to develop software.

Which of the following SDLC phases meets the audit objectives defined below: System and data are validated. System meets all user requirements. System meets all control requirements.

- A. Evaluation and acceptance
- B. Programming and training
- C. Definition
- D. Initiation

Answer: A ([LEAVE A REPLY](#))

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: 67

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](#))

Explanation/Reference:

Explanation: 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: 68

Which of the following is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in business continuity?

- A. RTO
- B. RTA
- C. RPO
- D. RCO

Answer: A (LEAVE A REPLY)

The Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster or disruption in order to avoid unacceptable consequences associated with a break in business continuity. It includes the time for trying to fix the problem without a recovery, the recovery itself, tests and the communication to the users. Decision time for user representative is not included. The business continuity timeline usually runs parallel with an incident management timeline and may start at the same, or different, points. In accepted business continuity planning methodology, the RTO is established during the Business Impact Analysis (BIA) by the owner of a process (usually in conjunction with the Business Continuity planner). The RTOs are then presented to senior management for acceptance. The RTO attaches to the business process and not the resources required to support the process. Answer B is incorrect. The Recovery Time Actual (RTA) is established during an exercise, actual event, or predetermined based on recovery methodology the technology support team develops. This is the time frame the technology support takes to deliver the recovered infrastructure to the business. Answer D is incorrect. The Recovery Consistency Objective (RCO) is used in Business Continuity Planning in addition to Recovery Point Objective (RPO) and Recovery Time Objective (RTO). It applies data consistency objectives to Continuous Data Protection services. Answer C is incorrect. The Recovery Point Objective (RPO) describes the acceptable amount of data loss measured in time. It is the point in time to which data must be recovered as defined by the organization. The RPO is generally a definition of what an organization determines is an "acceptable loss" in a disaster situation. If the RPO of a company is 2 hours and the time it takes to get the data back into production is 5 hours, the RPO is still 2 hours. Based on this RPO the data must be restored to within 2 hours of the disaster.

NEW QUESTION: 69

Adam works as a Computer Hacking Forensic Investigator for a garment company in the United States. A project has been assigned to him to investigate a case of a disloyal employee who is suspected of stealing design of the garments, which belongs to the company and selling those garments of the same design under different brand name. Adam investigated that the company does not have any policy related to the copy of design of the garments. He also investigated that the trademark under which the employee is selling the garments is almost identical to the original trademark of the company. On the grounds of which of the following laws can the employee be prosecuted?

- A. Espionage law

- B. Trademark law
- C. Cyber law
- D. Copyright law

Answer: ([SHOW ANSWER](#))

The Trademark law is a piece of legislation that contains the federal statutes of trademark law in the United States. The Act prohibits a number of activities, including trademark infringement, trademark dilution, and false advertising. Trademarks were traditionally protected in the United States only under State common law, growing out of the tort of unfair competition. Trademark law in the United States is almost entirely enforced through private lawsuits. The exception is in the case of criminal counterfeiting of goods. Otherwise, the responsibility is entirely on the mark owner to file suit in either state or federal civil court in order to restrict an infringing use. Failure to "police" a mark by stopping infringing uses can result in the loss of protection. Answer D is incorrect. Copyright law of the United States governs the legally enforceable rights of creative and artistic works under the laws of the United States. Copyright law in the United States is part of federal law, and is authorized by the U.S. Constitution. The power to enact copyright law is granted in Article I, Section 8, Clause 8, also known as the Copyright Clause. This clause forms the basis for U.S. copyright law ("Science", "Authors", "Writings") and patent law ("useful Arts", "Inventors", "Discoveries"), and includes the limited terms (or durations) allowed for copyrights and patents ("limited Times"), as well as the items they may protect. In the U.S., registrations of claims of copyright, recordation of copyright transfers, and other administrative aspects of copyright are the responsibility of the United States Copyright Office, a part of the Library of Congress. Answer A is incorrect. The Espionage Act of 1917 was a United States federal law passed shortly after entering World War I, on June 15, 1917, which made it a crime for a person: To convey information with intent to interfere with the operation or success of the armed forces of the United States or to promote the success of its enemies. This was punishable by death or by imprisonment for not more than 30 years. To convey false reports or false statements with intent to interfere with the operation or success of the military or naval forces of the United States or to promote the success of its enemies and whoever when the United States is at war, to cause or attempt to cause insubordination, disloyalty, mutiny, refusal of duty, in the military or naval forces of the United States, or to willfully obstruct the recruiting or enlistment service of the United States. Answer C is incorrect. Cyber law is a very wide term, which wraps up the legal issue related to the use of communicative, transactional and distributive aspect of networked information device and technologies. It is commonly known as INTERNET LAW. These Laws are important to apply as Internet does not tend to make any geographical and jurisdictional boundaries clear; this is the reason why Cyber law is not very efficient. A single transaction may involve the laws of at least three jurisdictions, which are as follows: 1.The laws of the state/nation in which the user resides 2.The laws of the state/nation that apply where the server hosting the transaction is located 3.The laws of the state/nation, which apply to the person or business with whom the transaction takes place

NEW QUESTION: 70

Harry is the project manager of the MMQ Construction Project. In this project, Harry has identified a supplier who can create stained glass windows for 1,000 window units in the construction project. The supplier is an artist who works by himself, but creates windows for several companies throughout the United States. Management reviews the proposal to use this supplier and while they agree that the supplier is talented, they do not think the artist can fulfill the 1,000 window units in time for the project's deadline. Management asked Harry to find a supplier who can fulfill the completion of the windows by the needed date in the schedule. What risk response has management asked Harry to implement?

- A. Transference
- B. Avoidance
- C. Mitigation
- D. Acceptance

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation: This is an example of mitigation. By changing to a more reliable supplier, Harry is reducing the probability the supplier will be late. It's still possible that the vendor may not be able to deliver the stained glass windows, but the more reputable supplier reduces the probability of the lateness. Mitigation is a risk response planning technique associated with threats that seeks to reduce the probability of occurrence or impact of a risk to below an acceptable threshold. Risk mitigation involves taking early action to reduce the probability and impact of a risk occurring on the project. Adopting less complex processes, conducting more tests, or choosing a more stable supplier are examples of mitigation actions.

AnswerA is incorrect. Transference is when the risk is transferred to a third party, usually for a fee. While

this question does include a contractual relationship, the risk is the lateness of the windows.

Transference focuses on transferring the risk to a third party to manage the risk event. In this instance, the management of the risk is owned by a third party; the third party actually creates the risk event because of the possibility of the lateness of the windows. AnswerB is incorrect.

Avoidance changes the project plan to avoid the risk. If the project manager and management changed the window-type to a standard window in the project requirements, then this would be avoidance. Risk avoidance is a technique used for threats. It creates changes to the project management plan that are meant to either eliminate the risk completely or to protect the project objectives from its impact. Risk avoidance removes the risk event entirely either by adding additional steps to avoid the event or reducing the project scope requirements. It may seem the answer to all possible risks, but avoiding risks also means losing out on the potential gains that accepting (retaining) the risk might have allowed. AnswerD is incorrect. Acceptance accepts the risk that the windows could be late and offers no response.

NEW QUESTION: 71

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

- A. Valuations of the critical assets in hard costs.
- B. Evaluate potential threats to the assets.
- C. Estimate the potential losses to assets by determining their value.
- D. Establish the threats likelihood and regularity.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

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

NEW QUESTION: 72

Software Development Life Cycle (SDLC) is a logical process used by programmers to develop software. Which of the following SDLC phases meets the audit objectives defined below: System and data are validated. System meets all user requirements. System meets all control requirements.

- A. Evaluation and acceptance
- B. Programming and training
- C. Definition
- D. Initiation

Answer: A ([LEAVE A REPLY](#))

It is the evaluation and acceptance phase of the SDLC, which meets the following audit objectives: System and data are validated. System meets all user requirements. System meets all control requirements Answer D is incorrect. During the initiation phase, the need for a system is expressed and the purpose of the system is documented. Answer C is incorrect. During the definition phase, users' needs are defined and the needs are translated into requirements statements that incorporate appropriate controls. Answer B is incorrect. During the programming and training phase, the software and other components of the system are faithfully incorporated into the design specifications. Proper documentation and training are provided in this phase.

NEW QUESTION: 73

What are the various benefits of a software interface according to the "Enhancing the Development Life Cycle to Produce Secure Software" document? Each correct answer represents a complete solution.

Choose three.

- A. It modifies the implementation of a component without affecting the specifications of the interface.
- B. It controls the accessing of a component.
- C. It displays the implementation details of a component.
- D. It provides a programmatic way of communication between the components that are working with different programming languages.

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

Explanation/Reference:

Explanation: The benefits of a software interface are as follows: It provides a programmatic way of communication between the components that are working with different programming languages. It prevents direct communication between components. It modifies the implementation of a component without affecting the specifications of the interface. It hides the implementation details of a component. It controls the accessing of a component. Answer C is incorrect. A software interface hides the implementation details of the component.

NEW QUESTION: 74

You are responsible for network and information security at a metropolitan police station. The most important concern is that unauthorized parties are not able to access data. What is this called?

- A. Confidentiality
- B. Availability
- C. Integrity
- D. Encryption

Answer: A (LEAVE A REPLY)

The CIA (Confidentiality, Integrity, and Availability) triangle is concerned with three facets of security. Confidentiality is the concern that data be secure from unauthorized access. Answer B and C are incorrect. The CIA (Confidentiality, Integrity, and Availability) triangle is concerned with three facets of security. Integrity is the concern that data not be altered without it being traceable. Availability is the concern that the data, while being secured, is readily accessible. Answer D is incorrect. Confidentiality may be implemented with encryption but encryption is just a technique to obtain confidentiality.

NEW QUESTION: 75

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)

Explanation/Reference:

Explanation: 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: 76

Which of the following governance bodies provides management, operational and technical controls to satisfy security requirements?

- A. Senior Management
- B. Business Unit Manager
- C. Information Security Steering Committee
- D. Chief Information Security Officer

Answer: A (LEAVE A REPLY)

Senior management provides management, operational and technical controls to satisfy security requirements. The governance roles and responsibilities are mentioned below in the table:

Valid CSSLP Dumps shared by TrainingDump.com for Helping Passing CSSLP Exam! TrainingDump.com now offer the **newest CSSLP exam dumps**, the TrainingDump.com CSSLP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CSSLP dumps with Test Engine here:
<https://www.trainingdump.com/ISC/CSSLP-practice-exam-dumps.html> (349 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 77

The Systems Development Life Cycle (SDLC) is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems. Which of the following are the different phases of system development life cycle? Each correct answer represents a complete solution. Choose all that apply.

- A. Testing
- B. Implementation
- C. Operation/maintenance
- D. Development/acquisition
- E. Disposal
- F. Initiation

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

The Systems Development Life Cycle (SDLC), or Software Development Life Cycle in systems engineering, information systems, and software engineering, is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems. The concept generally refers to computers or information systems. The following are the five phases in a generic System Development Life Cycle: 1.Initiation 2.Development/acquisition 3.Implementation 4.Operation/maintenance 5.Disposal

NEW QUESTION: 78

Which of the following are the common roles with regard to data in an information classification program? Each correct answer represents a complete solution. Choose all that apply.

- A. Editor
- B. Custodian
- C. Owner
- D. User
- E. Security auditor

Answer: ([SHOW ANSWER](#))

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

NEW QUESTION: 79

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: B ([LEAVE A REPLY](#))

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: 80

Which of the following phases of the DITSCAP C&A process is used to define the C&A level of effort, to identify the main C&A roles and responsibilities, and to create an agreement on the method for implementing the security requirements?

- A. Phase 1
- B. Phase 4
- C. Phase 2
- D. Phase 3

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: The Phase 1 of the DITSCAP C&A process is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. Answer C is incorrect. The Phase 2 of the DITSCAP C&A process is known as Verification. Answer: D is incorrect. The Phase 3 of the DITSCAP C&A process is known as Validation. Answer: B is incorrect. The Phase 4 of the DITSCAP C&A process is known as Post Accreditation.

NEW QUESTION: 81

The NIST Information Security and Privacy Advisory Board (ISPAB) paper "Perspectives on Cloud Computing and Standards" specifies potential advantages and disadvantages of virtualization. Which of the following disadvantages does it include? Each correct answer represents a complete solution. Choose all that apply.

- A. It increases capabilities for fault tolerant computing using rollback and snapshot features.
- B. It increases intrusion detection through introspection.
- C. It initiates the risk that malicious software is targeting the VM environment.
- D. It increases overall security risk shared resources.
- E. It creates the possibility that remote attestation may not work.
- F. It involves new protection mechanisms for preventing VM escape, VM detection, and VM-VM interference.
- G. It increases configuration effort because of complexity and composite system.

Answer: ([SHOW ANSWER](#))

The potential security disadvantages of virtualization are as follows: It increases configuration effort because of complexity and composite system. It initiates the problem of how to prevent overlap while mapping VM storage onto host files. It introduces the problem of virtualizing the TPM. It creates the possibility that remote attestation may not work. It initiates the problem of

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

NEW QUESTION: 82

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: ([SHOW ANSWER](#))

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: 83

Which of the following policies can explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations?

- A. Informative
- B. Advisory
- C. Selective
- D. Regulatory

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: An informative policy informs employees about certain topics. It is not an enforceable policy, but rather one to teach individuals about specific issues relevant to the

company. The informative policy can explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations. AnswerD is incorrect. A regulatory policy ensures that an organization follows the standards set by specific industry regulations. This type of policy is very detailed and specific to a type of industry. The regulatory policy is used in financial institutions, health care facilities, public utilities, and other government-regulated industries, e.g., TRAI. Answer: B is incorrect. An advisory policy strongly advises employees regarding which types of behaviors and activities should and should not take place within the organization. It also outlines possible ramifications if employees do not comply with the established behaviors and activities. The advisory policy can be used to describe how to handle medical information, handle financial transactions, and process confidential information. Answer: C is incorrect. It is not a valid type of policy.

NEW QUESTION: 84

Which of the following statements describe the main purposes of a Regulatory policy? Each correct answer represents a complete solution. Choose all that apply.

- A.** It acknowledges the importance of the computing resources to the business model
- B.** It provides a statement of support for information security throughout the enterprise
- C.** It ensures that an organization is following the standard procedures or base practices of operation in its specific industry.
- D.** It gives an organization the confidence that it is following the standard and accepted industry policy.

Answer: C,D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: The main purposes of a Regulatory policy are as follows: It ensures that an organization is following the standard procedures or base practices of operation in its specific industry. It gives an organization the confidence that it is following the standard and accepted industry policy. AnswerB and A are incorrect. These are the policy elements of Senior Management Statement of Policy.

NEW QUESTION: 85

Which of the following DITSCAP phases validates that the preceding work has produced an IS that operates in a specified computing environment?

- A.** Phase 2
- B.** Phase 4
- C.** Phase 1
- D.** Phase 3

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation: The Phase 3 of DITSCAP C&A is known as Validation. The goal of Phase 3 is to validate that the preceding work has produced an IS that operates in a specified computing environment. AnswerC is incorrect. The goal of this phase is to define the C&A level of effort,

identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements.

Answer A is incorrect. The goal of this phase is to obtain a fully integrated system for certification testing

and accreditation. Answer B is incorrect. This phase ensures that it will maintain an acceptable level of residual risk.

NEW QUESTION: 86

Which of the following activities are performed by the 'Do' cycle component of PDCA (plan-do-check-act)?

Each correct answer represents a complete solution. Choose all that apply.

- A.** It detects and responds to incidents properly.
- B.** It determines controls and their objectives.
- C.** It manages resources that are required to achieve a goal.
- D.** It performs security awareness training.
- E.** It operates the selected controls.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

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

NEW QUESTION: 87

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

- A.** Quantitative risk analysis
- B.** Risk identification
- C.** Risk response implementation
- D.** Qualitative risk analysis

Answer: A ([LEAVE A REPLY](#))

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

NEW QUESTION: 88

Which of the following are the goals of risk management? Each correct answer represents a complete solution. Choose three.

- A. Identifying the risk
- B. Assessing the impact of potential threats
- C. Identifying the accused
- D. Finding an economic balance between the impact of the risk and the cost of the countermeasure

Answer: ([SHOW ANSWER](#))

There are three goals of risk management as follows: Identifying the risk Assessing the impact of potential threats Finding an economic balance between the impact of the risk and the cost of the countermeasure Answer C is incorrect. Identifying the accused does not come under the scope of risk management.

NEW QUESTION: 89

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

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

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. AnswerD is incorrect. The human resources management plan does define how risks will be analyzed.

Answer: B is incorrect. The staffing management plan does define how risks will be analyzed.

Answer: A is incorrect. The risk analysis plan does define how risks will be analyzed.

NEW QUESTION: 90

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
- G. 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.

Answer: B (LEAVE A REPLY)

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: 91

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)

When an attacker successfully inserts an intermediary software or program between two communicating hosts, it is known as man-in-the-middle attack.

Valid CSSLP Dumps shared by TrainingDump.com for Helping Passing CSSLP Exam! TrainingDump.com now offer the **newest CSSLP exam dumps**, the TrainingDump.com CSSLP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CSSLP dumps with Test Engine here:

<https://www.trainingdump.com/ISC/CSSLP-practice-exam-dumps.html> (349 Q&As Dumps,

40%OFF Special Discount: Exam-Tests)

NEW QUESTION: 92

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

- A. Compliance control
- B. Physical control

C. Procedural control

D. Technical control

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

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

NEW QUESTION: 93

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

A. What is being secured?

B. Where is the vulnerability, threat, or risk?

C. Who is expected to exploit the vulnerability?

D. Who is expected to comply with the policy?

Answer: A,B,D ([LEAVE A REPLY](#))

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

NEW QUESTION: 94

The Data and Analysis Center for Software (DACS) specifies three general principles for software assurance which work as a framework in order to categorize various secure design principles. Which of the following principles and practices does the General Principle 1 include? Each correct answer represents a complete solution. Choose two.

A. Principle of separation of privileges, duties, and roles

B. Assume environment data is not trustworthy

C. Simplify the design

D. Principle of least privilege

Answer: A,D ([LEAVE A REPLY](#))

General Principle 1- Minimize the number of high-consequence targets includes the following principles and practices: Principle of least privilege Principle of separation of privileges, duties, and roles Principle of separation of domains Answer B is incorrect. Assume environment data is

not trustworthy principle is included in the General Principle 2. Answer C is incorrect. Simplify the design principle is included in the General Principle 3.

NEW QUESTION: 95

Which of the following types of obfuscation transformation increases the difficulty for a de-obfuscation tool so that it cannot extract the true application from the obfuscated version?

- A.** Preventive transformation
- B.** Data obfuscation
- C.** Control obfuscation
- D.** Layout obfuscation

Answer: A ([LEAVE A REPLY](#))

Preventive transformation increases the difficulty for a de-obfuscation tool so that it cannot extract the true application from the obfuscated version.

NEW QUESTION: 96

Which of the following types of redundancy prevents attacks in which an attacker can get physical control of a machine, insert unauthorized software, and alter data?

- A.** Data redundancy
- B.** Hardware redundancy
- C.** Process redundancy
- D.** Application redundancy

Answer: ([SHOW ANSWER](#)**)**

Process redundancy permits software to run simultaneously on multiple geographically distributed locations, with voting on results. It prevents attacks in which an attacker can get physical control of a machine, insert unauthorized software, and alter data.

NEW QUESTION: 97

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: 98

You and your project team have identified the project risks and now are analyzing the probability and impact of the risks. What type of analysis of the risks provides a quick and high-level review of each identified risk event?

- A. Quantitative risk analysis
- B. Qualitative risk analysis
- C. Seven risk responses
- D. A risk probability-impact matrix

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: Qualitative risk analysis is a high-level, fast review of the risk event. Qualitative risk analysis qualifies the risk events for additional analysis.

NEW QUESTION: 99

Which of the following phases of the DITSCAP C&A process is used to define the C&A level of effort, to identify the main C&A roles and responsibilities, and to create an agreement on the method for implementing the security requirements?

- A. Phase 1
- B. Phase 4
- C. Phase 2
- D. Phase 3

Answer: ([SHOW ANSWER](#))

The Phase 1 of the DITSCAP C&A process is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. Answer C is incorrect. The Phase 2 of the DITSCAP C&A process is known as Verification. Answer D is incorrect. The Phase 3 of the DITSCAP C&A process is known as Validation. Answer B is incorrect. The Phase 4 of the DITSCAP C&A process is known as Post Accreditation.

NEW QUESTION: 100

Which of the following are the basic characteristics of declarative security? Each correct answer represents a complete solution. Choose all that apply.

- A. It is a container-managed security.
- B. It has a runtime environment.
- C. All security constraints are stated in the configuration files.
- D. The security policies are applied at the deployment time.

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation: The following are the basic characteristics of declarative security: In declarative security, programming is not required. All security constraints are stated in the configuration files. It is a container- managed security. The application server manages the enforcing process of security constraints. It has a runtime environment. The security policies for runtime environment are represented by the deployment descriptor. It can support different environments, such as development, testing, and production. AnswerD is incorrect. It is the characteristic of programmatic security.

NEW QUESTION: 101

Which of the following approaches can be used to build a security program? Each correct answer represents a complete solution. Choose all that apply.

- A. Right-Up Approach
- B. Left-Up Approach
- C. Top-Down Approach
- D. Bottom-Up Approach

Answer: C,D (LEAVE A REPLY)

Explanation/Reference:

Explanation: Top-Down Approach is an approach to build a security program. The initiation, support, and direction come from the top management and work their way through middle management and then to staff members. It is treated as the best approach. This approach ensures that the senior management, who is ultimately responsible for protecting the company assets, is driving the program. Bottom-Up Approach is an approach to build a security program. The lower-end team comes up with a security control or a program without proper management support and direction. It is less effective and doomed to fail. Answer:

A and B are incorrect. No such types of approaches exist

NEW QUESTION: 102

The NIST ITL Cloud Research Team defines some primary and secondary technologies as the fundamental elements of cloud computing in its "Effectively and Securely Using the Cloud Computing Paradigm" presentation. Which of the following technologies are included in the primary technologies?

Each correct answer represents a complete solution. Choose all that apply.

- A. Web application framework
- B. Free and open source software
- C. SOA
- D. Virtualization

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

Explanation/Reference:

Explanation: The primary technologies defined by the NIST ITL Cloud Research Team in its "Effectively and Securely Using the Cloud Computing Paradigm" presentation are as follows: Virtualization Grid technology SOA (Service Oriented Architecture) Distributed computing Broadband network Browser as a platform Free and open source software Answer A is incorrect. It is defined as the secondary technology.

NEW QUESTION: 103

Which of the following processes identifies the threats that can impact the business continuity of operations?

- A.** Function analysis
- B.** Risk analysis
- C.** Business impact analysis
- D.** Requirement analysis

Answer: C (LEAVE A REPLY)

A business impact analysis (BIA) is a crisis management and business impact analysis technique that identifies those threats that can impact the business continuity of operations. Such threats can be either natural or man-made. The BIA team should have a clear understanding of the organization, key business processes, and IT resources for assessing the risks associated with continuity. In the BIA team, there should be senior management, IT personnel, and end users to identify all resources that are to be used during normal operations. Answer B is incorrect. Risk analysis is the science of risks and their probability and evaluation in a business or a process. It is an important factor in security enhancement and prevention in a system. Risk analysis should be performed as part of the risk management process for each project. The outcome of the risk analysis would be the creation or review of the risk register to identify and quantify risk elements to the project and their potential impact. Answer A is incorrect. The functional analysis process is used for converting system requirements into a comprehensive function standard. Verification is the result of the functional analysis process, in which the fundamentals of a system level functional architecture are defined adequately to allow for synthesis in the design phase. The functional analysis breaks down the higher-level functions into the lower level functions. Answer D is incorrect. Requirements analysis encompasses the tasks that go into determining the needs or conditions to meet for a new or altered product, taking account of the possibly conflicting requirements of the various stakeholders.

NEW QUESTION: 104

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](#))

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. Answer A 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: 105

Which of the following elements of the BCP process emphasizes on creating the scope and the additional elements required to define the parameters of the plan?

- A.** Business continuity plan development
- B.** Plan approval and implementation
- C.** Business impact analysis
- D.** Scope and plan initiation

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: The scope and plan initiation process in BCP symbolizes the beginning of the BCP process. It emphasizes on creating the scope and the additional elements required to define the parameters of the plan. The scope and plan initiation phase embodies a check of the company's operations and support services. The scope activities include creating a detailed account of the work required, listing the resources to be used, and defining the management practices to be employed. Answer C is incorrect. The business impact assessment is a method used to facilitate business units to understand the impact of a disruptive event. This phase includes the execution of a vulnerability assessment. This process makes out the mission-critical areas and business processes that are important for the survival of business. It is similar to the risk assessment

process. The function of a business impact assessment process is to create a document, which is used to help and understand what impact a disruptive event would have on the business.

Answer A is incorrect. The business continuity plan development refers to the utilization of the information

collected in the Business Impact Analysis (BIA) for the creation of the recovery strategy plan to support the critical business functions. The information gathered from the BIA is mapped out to make a strategy for creating a continuity plan. The business continuity plan development process includes the areas of plan implementation, plan testing, and ongoing plan maintenance. This phase also consists of defining and documenting the continuity strategy. Answer B is incorrect. The plan approval and implementation process involves creating enterprise-wide awareness of the plan, getting the final senior management signoff, and implementing a maintenance procedure for updating the plan as required.

NEW QUESTION: 106

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

- A. Availability
- B. Confidentiality
- C. Non repudiation
- D. Data Protection

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

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

Valid CSSLP Dumps shared by TrainingDump.com for Helping Passing CSSLP Exam! TrainingDump.com now offer the **newest CSSLP exam dumps**, the TrainingDump.com CSSLP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CSSLP dumps with Test Engine here:

<https://www.trainingdump.com/ISC/CSSLP-practice-exam-dumps.html> (349 Q&As Dumps,

40%OFF Special Discount: Exam-Tests)

NEW QUESTION: 107

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](#))

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. Answer B is incorrect. Accountability determines

the actions and behaviors of an individual within a system, and identifies that particular individual.

Audit trails and logs support accountability.

NEW QUESTION: 108

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: ([SHOW ANSWER](#))

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: 109

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: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: 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, screw-

drivers 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: 110

Elizabeth is a project manager for her organization and she finds risk management to be very difficult for her to manage. She asks you, a lead project manager, at what stage in the project will risk management become easier. What answer best resolves the difficulty of risk management practices and the effort required?

- A. Risk management only becomes easier when the project moves into project execution.
- B. Risk management only becomes easier when the project is closed.
- C. Risk management is an iterative process and never becomes easier.
- D. Risk management only becomes easier the more often it is practiced.

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: According to the PMBOK, "Like many things in project management, the more it is done the easier the practice becomes." AnswerB is incorrect. This answer is not the best choice for the project.

AnswerA is incorrect. Risk management likely becomes more difficult in project execution than in other

stages of the project. AnswerC is incorrect. Risk management does become easier the more often it is done.

NEW QUESTION: 111

Which of the following statements best describes the difference between the role of a data owner and the role of a data custodian?

- A. The custodian makes the initial information classification assignments, and the operations manager implements the scheme.
- B. The data owner implements the information classification scheme after the initial assignment by the custodian.
- C. The custodian implements the information classification scheme after the initial assignment by the operations manager.
- D. The data custodian implements the information classification scheme after the initial assignment by the data owner.

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: The data owner is responsible for ensuring that the appropriate security controls are in place, for assigning the initial classification to the data to be protected, for approving access requests from other parts of the organization, and for periodically reviewing the data classifications and access rights. Data owners are primarily responsible for determining the data's sensitivity or classification levels, whereas the data custodian has the responsibility for backup, retention, and recovery of data. The data owner delegates these responsibilities to the custodian.

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

NEW QUESTION: 112

You work as a CSO (Chief Security Officer) for Tech Perfect Inc. You want to perform the following tasks:

Develop a risk-driven enterprise information security architecture. Deliver security infrastructure solutions that support critical business initiatives. Which of the following methods will you use to accomplish these tasks?

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

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

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

The service-oriented architecture (SOA) is a flexible set of design principles used during the phases of systems development and integration.

NEW QUESTION: 113

What are the subordinate tasks of the Implement and Validate Assigned IA Control phase in the DIACAP process? Each correct answer represents a complete solution. Choose all that apply.

- A. Conduct validation activities.
- B. Execute and update IA implementation plan.
- C. Combine validation results in DIACAP scorecard.
- D. Conduct activities related to the disposition of the system data and objects.

Answer: A,B,C ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for

managing risk. The subordinate tasks of the Implement and Validate Assigned IA Control phase in the DIACAP process are as follows: Execute and update IA implementation plan. Conduct validation activities. Combine validation results in the DIACAP scorecard. Answer D is incorrect. The activities related to the disposition of the system data and objects are conducted in the fifth phase of the DIACAP process. The fifth phase of the DIACAP process is known as Decommission System.

NEW QUESTION: 114

In which of the following alternative processing sites is the backup facility maintained in a constant order, with a full complement of servers, workstations, and communication links ready to assume the primary operations responsibility?

- A.** Cold Site
- B.** Hot Site
- C.** Warm Site
- D.** Mobile Site
- E.** Explanation:

A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data. It provides the backup facility, which is maintained in a constant order, with a full complement of servers, workstations, and communication links ready to assume the primary operations responsibility. A hot site is a backup site in case disaster has taken place in a data center. A hot site is located off site and provides the best protection. It is an exact replica of the current data center. In case a disaster struck to the data center, administrators just need to take the backup of recent data in hot site and the data center is back online in a very short time. It is very expensive to create and maintain the hot site. There are lots of third party companies that provide disaster recovery solutions by maintaining hot sites at their end.

Answer: B (LEAVE A REPLY)

is incorrect. A cold site is a backup site in case disaster has taken place in a data center. This is the least expensive disaster recovery solution, usually having only a single room with no equipment. All equipment is brought to the site after the disaster. It can be on site or off site. Answer D is incorrect. Mobile sites are self-reliant, portable shells custom-fitted with definite telecommunications and IT equipment essential to meet system requirements. These are presented for lease through commercial vendors. Answer C is incorrect. A warm site is, quite logically, a compromise between hot and cold sites. Warm sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. These sites will have backups on hand, but they may not be complete and may be between several days and a week old. An example would be backup tapes sent to the warm site by courier.

NEW QUESTION: 115

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 Fraggles Trinoo Tribe Flood Network

NEW QUESTION: 116

Which of the following is an open source network intrusion detection system?

- A. NETSH
- B. Macof
- C. Sourcefire
- D. Snort
- E. Explanation:

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: D,E (LEAVE A REPLY)

is incorrect. Macof is a tool of the dsniff tool set and used to flood the local network with random MAC addresses. It causes some switches to fail open in repeating mode, and facilitates sniffing. Answer C is incorrect. Sourcefire is the company that owns and maintains Snort. Answer A is incorrect. NETSH is not a network intrusion detection system. NETSH is a command line tool to

configure TCP/IP settings such as the IP address, Subnet Mask, Default Gateway, DNS, WINS addresses, etc.

NEW QUESTION: 117

There are seven risks responses that a project manager can choose from. Which risk response is appropriate for both positive and negative risk events?

- A.** Acceptance
- B.** Transference
- C.** Sharing
- D.** Mitigation

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: Only acceptance is appropriate for both positive and negative risk events. Often sharing is used for low probability and low impact risk events regardless of the positive or negative effects the risk event may bring the project. Acceptance response is a part of Risk Response planning process.

Acceptance response delineates that the project plan will not be changed to deal with the risk. Management may develop a contingency plan if the risk does occur. Acceptance response to a risk event is a strategy that can be used for risks that pose either threats or opportunities.

Acceptance response can be of two types: Passive acceptance: It is a strategy in which no plans are made to try or avoid or mitigate the risk. Active acceptance: Such responses include developing contingency reserves to deal with risks, in case they occur. Acceptance is the only response for both threats and opportunities. Answer: C is incorrect. Sharing is a positive risk response that shares an opportunity for all parties involved in the risk event. Answer: B is incorrect. Transference is a negative risk event that transfers the risk ownership to a third party, such as vendor, through a contractual relationship. Answer: D is incorrect. Mitigation is a negative risk event that seeks to lower the probability and/or impact of a risk event.

NEW QUESTION: 118

Which of the following are the responsibilities of a custodian with regard to data in an information classification program? Each correct answer represents a complete solution. Choose three.

- A.** Performing data restoration from the backups when necessary
- B.** Running regular backups and routinely testing the validity of the backup data
- C.** Determining what level of classification the information requires
- D.** Controlling access, adding and removing privileges for individual users

Answer: ([SHOW ANSWER](#)**)**

The owner of information delegates the responsibility of protecting that information to a custodian. The following are the responsibilities of a custodian with regard to data in an information classification program: Running regular backups and routinely testing the validity of the backup data Performing data restoration from the backups when necessary Controlling access, adding

and removing privileges for individual users Answer C is incorrect. Determining what level of classification the information requires is the responsibility of the owner.

NEW QUESTION: 119

John works as a systems engineer for BlueWell Inc. He has modified the software, and wants to retest the application to ensure that bugs have been fixed or not. Which of the following tests should John use to accomplish the task?

- A. Reliability test
- B. Functional test
- C. Performance test
- D. Regression test

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: John should use the regression tests to retest the application to guarantee that bugs have been fixed. This test will help him to check that the earlier working functions have not failed as a result of the changes, and newly added features have not created problems with the previous versions. 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: 120

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: A,B,D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: The vulnerability, port, and network scanning tools are used in penetration testing.

Vulnerability scanning is a process in which a Penetration Tester uses various tools to assess computers, computer systems, networks or applications for weaknesses. There are a number of types of vulnerability scanners available today, distinguished from one another by a focus on particular targets. While functionality varies between different types of vulnerability scanners, they share a common, core purpose of enumerating the vulnerabilities present in one or more targets.

Vulnerability scanners are a core technology component of Vulnerability management. Port scanning is the first basic step to get the details of open ports on the target system. Port scanning

is used to find a hackable server with a hole or vulnerability. A port is a medium of communication between two computers. Every service on a host is identified by a unique 16-bit number called a port. A port scanner is a piece of software designed to search a network host for open ports. This is often used by administrators to check the security of their networks and by hackers to identify running services on a host with the view to compromising it. Port scanning is used to find the open ports, so that it is possible to search exploits related to that service and application. Network scanning is a penetration testing activity in which a penetration tester or an attacker identifies active hosts on a network, either to attack them or to perform security assessment. A penetration tester uses various tools to identify all the live or responding hosts on the network and their corresponding IP addresses. AnswerC is incorrect. This option comes under vulnerability scanning.

NEW QUESTION: 121

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.

Answer:

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.

Valid CSSLP Dumps shared by TrainingDump.com for Helping Passing CSSLP Exam! TrainingDump.com now offer the **newest CSSLP exam dumps**, the TrainingDump.com CSSLP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CSSLP dumps with Test Engine here:
<https://www.trainingdump.com/ISC/CSSLP-practice-exam-dumps.html> (349 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 122

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: (SHOW ANSWER)

Explanation/Reference:

Explanation: 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. AnswerB 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. AnswerA 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: 123

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](#))

Explanation/Reference:

Explanation: 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: 124

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. What are the process activities of this phase?

Each correct answer represents a complete solution. Choose all that apply.

- A.** Certification analysis
- B.** Assessment of the Analysis Results
- C.** Configuring refinement of the SSAA
- D.** System development
- E.** Registration

Answer: A,B,C,D ([LEAVE A REPLY](#))

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. The process activities of this phase are as follows:

Configuring refinement of the SSAA System development Certification analysis Assessment of the Analysis Results Answer E is incorrect. Registration is a Phase 1 activity.

NEW QUESTION: 125

In which of the following cryptographic attacking techniques does an attacker obtain encrypted messages that have been encrypted using the same encryption algorithm?

- A.** Chosen plaintext attack
- B.** Chosen ciphertext attack
- C.** Ciphertext only attack
- D.** Known plaintext attack

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: In a ciphertext only attack, an attacker obtains encrypted messages that have been encrypted using the same encryption algorithm.

NEW QUESTION: 126

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: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: 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: 127

Which of the following security design patterns provides an alternative by requiring that a user's authentication credentials be verified by the database before providing access to that user's data?

- A.** Secure assertion
- B.** Authenticated session
- C.** Password propagation
- D.** Account logout

Answer: C ([LEAVE A REPLY](#))

Password propagation provides an alternative by requiring that a user's authentication credentials be verified by the database before providing access to that user's data. Answer D is incorrect. Account logout implements a limit on the incorrect password attempts to protect an account from automated password-guessing attacks. Answer B is incorrect. Authenticated session 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. Answer A is incorrect. Secure assertion distributes application-specific sanity checks throughout the system.

NEW QUESTION: 128

Which of the following policies can explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations?

- A.** Informative
- B.** Advisory
- C.** Selective
- D.** Regulatory

Answer: A ([LEAVE A REPLY](#))

An informative policy informs employees about certain topics. It is not an enforceable policy, but rather one to teach individuals about specific issues relevant to the company. The informative policy can explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations. Answer D is incorrect. A regulatory policy ensures that an organization follows the standards set by specific industry regulations. This type of policy is very detailed and specific to a type of industry. The regulatory policy is used in financial institutions, health care facilities, public utilities, and other government-regulated industries, e.g., TRAI. Answer B is incorrect. An advisory policy strongly advises employees regarding which types of behaviors and activities should and should not take place within the organization. It also outlines possible ramifications if employees do not comply with the established behaviors and activities. The advisory policy can be used to describe how to handle medical information, handle financial transactions, and process confidential information. Answer C is incorrect. It is not a valid type of policy.

NEW QUESTION: 129

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.

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 (issued 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: 130

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

- A. DIACAP
- B. SSAA
- C. DAA
- D. ISSO

Answer: A ([LEAVE A REPLY](#))

DIACAP describes a residual risk as the risk remaining after a risk mitigation has occurred. The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk. DIACAP replaced the former process, known as DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process), in 2006. DoD Instruction (DoDI) 8510.01 establishes a standard DoD-wide process with a set of activities, general tasks, and a management structure to certify and accredit an Automated Information System (AIS) that will maintain the Information Assurance (IA) posture of the Defense Information Infrastructure (DII) throughout the system's life cycle. DIACAP applies to the acquisition, operation, and sustainment

of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. It identifies four phases: 1. System Definition 2. Verification 3. Validation 4. Re-Accreditation Answer D is incorrect. An Information System Security Officer (ISSO) plays the role of a supporter. The responsibilities of an Information System Security Officer (ISSO) are as follows: Manages the security of the information system that is slated for Certification & Accreditation (C&A). Insures the information systems configuration with the agency's information security policy. Supports the information system owner/information owner for the completion of security-related responsibilities. Takes part in the formal configuration management process. Prepares Certification & Accreditation (C&A) packages. Answer C is incorrect. The Designated Approving Authority (DAA), in the United States Department of Defense, is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. The DAA is responsible for implementing system security. The DAA can grant the accreditation and can determine that the system's risks are not at an acceptable level and the system is not ready to be operational. Answer B is incorrect. System Security Authorization Agreement (SSAA) is an information security document used in the United States Department of Defense (DoD) to describe and accredit networks and systems. The SSAA is part of the Department of Defense Information Technology Security Certification and Accreditation Process, or DITSCAP (superseded by DIACAP). The DoD instruction (issues in December 1997, that describes DITSCAP and provides an outline for the SSAA document is DODI 5200.40. The DITSCAP application manual (DoD 8510.1-M), published in July 2000, provides additional details.

NEW QUESTION: 131

Which of the following is a name, symbol, or slogan with which a product is identified?

- A. Trademark
- B. Copyright
- C. Trade secret
- D. Patent

Answer: A ([LEAVE A REPLY](#))

A trademark is a name, symbol, or slogan with which a product is identified. Its uniqueness makes the product noticeable among the same type of products. For example, Pentium and Athlon are brand names of the CPUs that are manufactured by Intel and AMD, respectively. The trademark law protects a company's trademark by making it illegal for other companies to use it without taking prior permission of the trademark owner. A trademark is registered so that others cannot use identical or similar marks. Answer C is incorrect. 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 B 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 D is incorrect. A patent is a set of exclusive rights granted to anyone who invents any new and useful machine, process, composition of matter, etc. A patent enables the inventor to legally enforce his right to exclude others from using his invention.

NEW QUESTION: 132

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

- A.** IR Incident Response
- B.** Information systems acquisition, development, and maintenance
- C.** SA System and Services Acquisition
- D.** CA Certification, Accreditation, and Security Assessments

Answer: A,C,D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: 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: 133

You have a storage media with some data and you make efforts to remove this data. After performing this, you analyze that the data remains present on the media. Which of the following refers to the above mentioned condition?

- A.** Object reuse
- B.** Degaussing
- C.** Residual
- D.** Data remanence

Answer: D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: Data remanence refers to the data that remains even after the efforts have been made for removing or erasing the data. This event occurs because of data being left intact by an insignificant file deletion operation, by storage media reformatting, or through physical properties of the storage medium.

Data remanence can make unintentional disclosure of sensitive information possible. So, it is required that the storage media is released into an uncontrolled environment. Answer: C and B are incorrect. These are the made-up disasters. Answer: A is incorrect. Object reuse refers to reassigning some other object of a storage media that has one or more objects.

NEW QUESTION: 134

SIMULATION

Fill in the blank with an appropriate phrase. _____ is used to provide security mechanisms for the storage, processing, and transfer of data.

Answer:

Data classification

Explanation/Reference:

Explanation: 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: 135

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: 136

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.

Valid CSSLP Dumps shared by TrainingDump.com for Helping Passing CSSLP Exam! TrainingDump.com now offer the **newest CSSLP exam dumps**, the TrainingDump.com CSSLP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CSSLP dumps with Test Engine here:
<https://www.trainingdump.com/ISC/CSSLP-practice-exam-dumps.html> (349 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 137

Which of the following plans is a comprehensive statement of consistent actions to be taken before, during, and after a disruptive event that causes a significant loss of information systems resources?

- A. Contingency plan
- B. Continuity of Operations plan
- C. Disaster recovery plan
- D. Business Continuity plan

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: 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.

AnswerD 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. AnswerB 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. AnswerA 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: 138

In which of the following phases of the DITSCAP process does Security Test and Evaluation (ST&E) occur?

- A. Phase 2

- B. Phase 4
- C. Phase 3
- D. Phase 1

Answer: ([SHOW ANSWER](#))

Security Test and Evaluation (ST&E) occurs in Phase 3 of the DITSCAP C&A process. Answer D is incorrect. The Phase 1 of DITSCAP C&A is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. The Phase 1 starts with the input of the mission need. This phase comprises three process activities: Document mission need Registration Negotiation Answer A is incorrect. The Phase 2 of DITSCAP C&A is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. This phase takes place between the signing of the initial version of the SSAA and the formal accreditation of the system. This phase verifies security requirements during system development. The process activities of this phase are as follows: Configuring refinement of the SSAA System development Certification analysis Assessment of the Analysis Results Answer B is incorrect. The Phase 4 of DITSCAP C&A is known as Post Accreditation. This phase starts after the system has been accredited in the Phase 3. The goal of this phase is to continue to operate and manage the system and to ensure that it will maintain an acceptable level of residual risk. The process activities of this phase are as follows: System operations Security operations Maintenance of the SSAA Change management Compliance validation

NEW QUESTION: 139

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

- A. Classic information security model
- B. Five Pillars model
- C. Certification and Accreditation (C&A)
- D. Information Assurance (IA)

Answer: ([SHOW ANSWER](#))

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: 140

Henry is the project manager of the QBG Project for his company. This project has a budget of \$4,576,900 and is expected to last 18 months to complete. The CIO, a stakeholder in the project, has introduced a scope change request for additional deliverables as part of the project work. What component of the change control system would review the proposed changes' impact on the features and functions of the project's product?

- A.** Configuration management system
- B.** Scope change control system
- C.** Cost change control system
- D.** Integrated change control

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: The configuration management system ensures that proposed changes to the project's scope are reviewed and evaluated for their affect on the project's product. Configuration

Management System is a subsystem of the overall project management system. It is a collection of formal documented procedures used to identify and document the functional and physical characteristics of a product, result, service, or component of the project. It also controls any changes to such characteristics, and records and reports each change and its implementation status. It includes the documentation, tracking systems, and defined approval levels necessary for authorizing and controlling changes. Audits are performed as part of configuration management to determine if the requirements have been met. AnswerB is incorrect. The scope change control system focuses on reviewing the actual changes to the project scope. When a change to the project's scope is proposed, the configuration management system is also invoked. Answer: C is incorrect. The cost change control system is responsible for reviewing and controlling changes to the project costs. AnswerD is incorrect. Integrated change control examines the affect of a proposed change on the project as a whole.

NEW QUESTION: 141

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](#))

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. 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: 142

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 emphasize 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: 143

The DARPA paper defines various procedural patterns to perform secure system development practices.

Which of the following patterns does it include? Each correct answer represents a complete solution.

Choose three.

- A. Hidden implementation
- B. Document the server configuration
- C. Patch proactively
- D. Red team the design
- E. Password propagation

Answer: B,C,D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: The following procedural patterns are defined by the DARPA paper in order to perform secure software development practices: Build the server from the ground up: It includes the following features:

Build the server from the ground up. Identify the default installation of the operating system and applications. Support hardening procedures to remove unnecessary services. Identify a vulnerable service for ongoing risk management. Choose the right stuff: It defines guidelines to select right commercial off- the-shelf (COTS) components and decide whether to use and build custom components. Document the server configuration: It supports the creation of an initial configuration baseline and tracks all modifications made to servers and application configurations.

Patch proactively: It supports in applying patches as soon as they are available rather than waiting until the systems cooperate. Red team the design: It supports an independent security assessment from the perspective of an attacker in the quality assurance or testing stage. An independent security assessment is helpful in addressing a security issue before it occurs.

AnswerA is incorrect. Hidden implementation pattern is not defined in the DARPA paper. This pattern is applicable to software assurance in general.

Hidden implementation limits the ability of an attacker to distinguish the internal workings of an application.

AnswerE is incorrect. Password propagation is not defined in the DARPA paper. This pattern is applicable

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

NEW QUESTION: 144

Which of the following activities are performed by the 'Do' cycle component of PDCA (plan-do-check-act)? Each correct answer represents a complete solution. Choose all that apply.

- A. It detects and responds to incidents properly.
- B. It determines controls and their objectives.
- C. It manages resources that are required to achieve a goal.
- D. It performs security awareness training.
- E. It operates the selected controls.

Answer: A,C,D,E ([LEAVE A REPLY](#))

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

NEW QUESTION: 145

The Systems Development Life Cycle (SDLC) is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems. Which of the following are the different phases of system development life cycle? Each correct answer represents a complete solution.

Choose all that apply.

- A. Testing
- B. Implementation
- C. Operation/maintenance
- D. Development/acquisition
- E. Disposal
- F. Initiation

Answer: B,C,D,E,F ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: The Systems Development Life Cycle (SDLC), or Software Development Life Cycle in systems engineering, information systems, and software engineering, is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems. The concept generally refers to computers or information systems. The following are the five phases in a generic System Development Life Cycle: 1.Initiation 2.Development/acquisition 3.Implementation 4.Operation/ maintenance 5.Disposal

NEW QUESTION: 146

Which of the following access control models uses a predefined set of access privileges for an object of a system?

- A. Role-Based Access Control
- B. Discretionary Access Control
- C. Policy Access Control
- D. Mandatory Access Control

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: Mandatory Access Control (MAC) is a model that uses a predefined set of access privileges for an object of the system. Access to an object is restricted on the basis of the sensitivity of the object and granted through authorization. Sensitivity of an object is defined by the label assigned to it. For example, if a user receives a copy of an object that is marked as "secret", he cannot grant permission to other users to see this object unless they have the

appropriate permission. AnswerB is incorrect. DAC is an access control model. In this model, the data owner has the right to decide who can access the data. Answer: A is incorrect. Role-based access control (RBAC) is an access control model. In this model, a user can access resources according to his role in the organization. For example, a backup administrator is responsible for taking backups of important data. Therefore, he is only authorized to access this data for backing it up.

However, sometimes users with different roles need to access the same resources. This situation can also be handled using the RBAC model. AnswerC is incorrect. There is no such access control model as Policy Access Control.

NEW QUESTION: 147

DRAG DROP

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

Select and Place:

Answer:

Explanation/Reference:

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: 148

Which of the following SDLC phases consists of the given security controls: Misuse Case Modeling Security Design and Architecture Review Threat and Risk Modeling Security Requirements and Test Cases Generation?

- A.** Deployment
- B.** Requirements Gathering
- C.** Maintenance
- D.** Design

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation: The various security controls in the SDLC design phase are as follows:

Misuse Case Modeling: It is important that the inverse of the misuse cases be modeled to understand and address the security aspects of the software. The requirements traceability matrix

can be used to track the misuse cases to the functionality of the software. Security Design and Architecture Review: This control can be introduced when the teams are engaged in the "functional" design and architecture review of the software. Threat and Risk Modeling: Threat modeling determines the attack surface of the software by examining its functionality for trust boundaries, data flow, entry points, and exit points. Risk modeling is performed by ranking the threats as they pertain to the users organization's business objectives, compliance and regulatory requirements and security exposures. Security Requirements and Test Cases Generation: All the above three security controls, i.e., Misuse Case Modeling, Security Design and Architecture Review, and Threat and Risk Modeling are used to produce the security requirements.

NEW QUESTION: 149

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

- A.** Quantitative risk analysis is the process of prioritizing risks for further analysis or action by assessing and combining their probability of occurrence and impact.
- B.** Quantitative risk analysis is the review of the risk events with the high probability and the highest impact on the project objectives.
- C.** Quantitative risk analysis is the planning and quantification of risk responses based on probability and impact of each risk event.
- D.** Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives.

Answer: D ([LEAVE A REPLY](#))

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

NEW QUESTION: 150

Part of your change management plan details what should happen in the change control system for your project. Theresa, a junior project manager, asks what the configuration management activities are for scope changes. You tell her that all of the following are valid configuration management activities except for which one?

- A.** Configuration Identification
- B.** Configuration Verification and Auditing
- C.** Configuration Status Accounting
- D.** Configuration Item Costing

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation: Configuration item cost is not a valid activity for configuration management. Cost changes are managed by the cost change control system; configuration management is concerned with changes to the features and functions of the project deliverables.

NEW QUESTION: 151

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: (SHOW ANSWER)

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.

Valid CSSLP Dumps shared by TrainingDump.com for Helping Passing CSSLP Exam! TrainingDump.com now offer the **newest CSSLP exam dumps**, the TrainingDump.com CSSLP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CSSLP dumps with Test Engine here:
<https://www.trainingdump.com/ISC/CSSLP-practice-exam-dumps.html> (349 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 152

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

- A. Copyright
- B. Snooping
- C. Utility model
- D. Patent

Answer: (SHOW ANSWER)

A patent is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention. Answer A is incorrect. A copyright is a form of intellectual property, which secures to its holder the exclusive right to produce copies of his or her works of original expression, such as a literary work, movie, musical work or sound recording, painting, photograph, computer program, or industrial design, for a defined, yet extendable, period of time. It does not cover ideas or facts. Copyright laws protect intellectual property from misuse by other individuals. Answer B is incorrect. Snooping is an activity of observing the content that appears on a computer monitor or watching what a user is typing. Snooping also occurs by using software programs to remotely monitor activity on a computer or network device. Hackers or attackers use snooping techniques and equipment such as keyloggers to monitor keystrokes, capture passwords and login information, and to intercept e-mail and other private communications. Sometimes, organizations also snoop their employees legitimately to monitor their use of organizations' computers and track Internet usage. Answer C is incorrect. A utility model is an intellectual property right to protect inventions.

NEW QUESTION: 153

Which of the following provides an easy way to programmers for writing lower-risk applications and retrofitting security into an existing application?

- A. Watermarking
- B. Code obfuscation
- C. Encryption wrapper
- D. ESAPI

Answer: D ([LEAVE A REPLY](#))

ESAPI (Enterprise Security API) is a group of classes that encapsulate the key security operations, needed by most of the applications. It is a free, open source, Web application security control library. ESAPI provides an easy way to programmers for writing lower-risk applications and retrofitting security into an existing application. It offers a solid foundation for new development. Answer C is incorrect. An encryption wrapper is a device that encrypts and decrypts the critical or all software codes at runtime. Answer B is incorrect. Code obfuscation transforms the code so that it is less intelligible for a person. Answer A is incorrect. Watermarking is the irreversible process of embedding information into a digital media. The purpose of digital watermarks is to provide copyright protection for intellectual property that is in digital form.

NEW QUESTION: 154

Which of the following terms refers to the protection of data against unauthorized access?

- A. Integrity
- B. Recovery
- C. Auditing
- D. Confidentiality

Answer: ([SHOW ANSWER](#)**)**

Explanation/Reference:

Explanation: Confidentiality is a term that refers to the protection of data against unauthorized access.

Administrators can provide confidentiality by encrypting data. Symmetric encryption is a relatively fast encryption method. Hence, this method of encryption is best suited for encrypting large amounts of data such as files on a computer. AnswerA is incorrect. Integrity ensures that no intentional or unintentional unauthorized modification is made to data. AnswerC is incorrect. Auditing is used to track user accounts for file and object access, logon attempts, system shutdown etc. This enhances the security of the network.

Before enabling auditing, the type of event to be audited should be specified in the Audit Policy in User Manager for Domains.

NEW QUESTION: 155

Which of the following is a patch management utility that scans one or more computers on a network and alerts a user if any important Microsoft security patches are missing and also provides links that enable those missing patches to be downloaded and installed?

- A. MABS
- B. ASNB
- C. MBSA
- D. IDMS

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: Microsoft Baseline Security Analyzer (MBSA) is a tool that includes a graphical and command line interface that can perform local or remote scans of Windows systems. It runs on computers running Windows 2000, Windows XP, or Windows Server 2003 operating system. MBSA scans for common security misconfigurations in Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, Internet Information Server (IIS) 4.0 and above, SQL Server 7.0 and 2000, and Office 2000 and 2002. It also scans for missing hot fixes in several Microsoft products, such as Windows 2000, Windows XP, SQL Server etc. AnswerB, D, and A are incorrect. These are invalid options.

NEW QUESTION: 156

In which of the following phases of the SDLC does the software and other components of the system faithfully incorporate the design specifications and provide proper documentation and training?

- A. Design
- B. Evaluation and acceptance
- C. Programming and training
- D. Initiation

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation: In the programming and training phase of the SDLC, the software and other components of the system faithfully incorporate the design specifications, and proper documentation and training are provided. AnswerD is incorrect. During the initiation phase, the need for a system is expressed and the purpose of the system is documented. Answer A is incorrect. During the design phase, systems requirements are incorporated into design. This phase specifies to include controls that support the auditing of the system. Answer: B is incorrect. During the evaluation and acceptance phase, the system and data are validated, all the control requirements and the user requirements are met by the system.

NEW QUESTION: 157

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)

Explanation/Reference:

Explanation: 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. AnswerB is incorrect.

Tamper evident specifies a process or device that makes unauthorized access to the protected object easily detected. AnswerD is incorrect. Tamper proofing makes computers resistant to interference.

Tamper proofing measures include automatic removal of sensitive information, automatic shutdown, and automatic physical locking. AnswerC is incorrect. Tamper data is used to view and modify the HTTP or HTTPS headers and post parameters.

NEW QUESTION: 158

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: 159

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: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: 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. AnswerC is incorrect. Non-disclosure agreements (NDAs) are often used to protect the confidentiality of an invention as it is being evaluated by potential licensees. AnswerD 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: 160

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](#))

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: 161

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: 162

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: 163

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

- A.** IR Incident Response
- B.** Information systems acquisition, development, and maintenance
- C.** SA System and Services Acquisition
- D.** CA Certification, Accreditation, and Security Assessments

Answer: **A,C,D** ([LEAVE A REPLY](#))

Following are the various U.S. Federal Government information security standards: AC Access Control AT Awareness and Training AU Audit and Accountability CA Certification, Accreditation, and Security Assessments CM Configuration Management CP Contingency Planning IA Identification and Authentication IR Incident Response MA Maintenance MP Media Protection PE Physical and Environmental Protection PL Planning PS Personnel Security RA Risk Assessment SA System and Services Acquisition SC System and Communications Protection SI System and Information Integrity Answer B is incorrect. Information systems acquisition, development, and maintenance is an International information security standard.

NEW QUESTION: 164

What component of the change management system is responsible for evaluating, testing, and documenting changes created to the project scope?

- A.** Project Management Information System
- B.** Integrated Change Control
- C.** Configuration Management System
- D.** Scope Verification

Answer: C ([LEAVE A REPLY](#))

The change management system is comprised of several components that guide the change request through the process. When a change request is made that will affect the project scope. The Configuration Management System evaluates the change request and documents the features and functions of the change on the project scope.

NEW QUESTION: 165

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 international information security standards? Each correct answer represents a complete solution. Choose all that apply.

- A. AU audit and accountability
- B. Human resources security
- C. Organization of information security
- D. Risk assessment and treatment

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: Following are the various international information security standards:

Risk assessment and treatment: Analysis of the organization's information security risks
Security policy:

Management direction
Organization of information security: Governance of information security

Asset management: Inventory and classification of information assets
Human resources security:

Security aspects for employees joining, moving, and leaving an organization
Physical and environmental security:

Protection of the computer facilities
Communications and operations management: Management of technical security controls in systems and networks
Access control: Restriction of access rights to networks, systems, applications, functions, and data

Information systems acquisition, development and maintenance: Building security into applications
Information security incident management: Anticipating and responding appropriately to information security breaches

Business continuity management:

Protecting, maintaining, and recovering business-critical processes and systems

Compliance: Ensuring conformance with information security policies, standards, laws, and regulations

Answer A is incorrect. AU audit and accountability is a U.S. Federal Government information security standard.

NEW QUESTION: 166

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

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

Answer: (SHOW ANSWER)

Configuration control is a procedure of the Configuration management. Configuration control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them. It supports the change of the functional and physical attributes of software at various points in time, and performs systematic control of changes to the identified attributes. Answer C is incorrect. Configuration audits confirm that the configuration identification for a configured item is accurate, complete, and will meet specified program needs. Configuration audits are broken into functional and physical configuration audits. They occur either at delivery or at the moment of effecting the change. A functional configuration audit ensures that functional and performance attributes of a configuration item are achieved, while a physical configuration audit ensures that a configuration item is installed in accordance with the requirements of its detailed design documentation. Answer D is incorrect. Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined. Baselining an attribute forces formal configuration change control processes to be effected in the event that these attributes are changed. Answer A is incorrect. The configuration status accounting procedure is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time. It supports the functional and physical attributes of software at various points in time, and performs systematic control of accounting to the identified attributes for the purpose of maintaining software integrity and traceability throughout the software development life cycle.

Valid CSSLP Dumps shared by TrainingDump.com for Helping Passing CSSLP Exam! TrainingDump.com now offer the **newest CSSLP exam dumps**, the TrainingDump.com CSSLP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CSSLP dumps with Test Engine here:

<https://www.trainingdump.com/ISC/CSSLP-practice-exam-dumps.html> (349 Q&As Dumps,

40%OFF Special Discount: Exam-Tests)

NEW QUESTION: 167

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](#))

Explanation/Reference:

Explanation: 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: 168

Which of the following is a patch management utility that scans one or more computers on a network and alerts a user if any important Microsoft security patches are missing and also provides links that enable those missing patches to be downloaded and installed?

- A. MABS
- B. ASNB
- C. MBSA
- D. IDMS

Answer: C ([LEAVE A REPLY](#))

Microsoft Baseline Security Analyzer (MBSA) is a tool that includes a graphical and command line interface that can perform local or remote scans of Windows systems. It runs on computers running Windows 2000, Windows XP, or Windows Server 2003 operating system. MBSA scans for common security misconfigurations in Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, Internet Information Server (IIS) 4.0 and above, SQL Server 7.0 and 2000, and Office 2000 and 2002. It also scans for missing hot fixes in several Microsoft products, such as Windows 2000, Windows XP, SQL Server etc. Answer B, D, and A are incorrect. These are invalid options.

NEW QUESTION: 169

According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Which of the following are among the eight areas of IA defined by DoD? Each correct answer represents a complete solution. Choose all that apply.

- A. VI Vulnerability and Incident Management
- B. Information systems acquisition, development, and maintenance
- C. DC Security Design & Configuration
- D. EC Enclave and Computing Environment

Answer: A,C,D ([LEAVE A REPLY](#))

According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Following are the various U.S. Department of Defense information security standards: DC Security Design & Configuration IA Identification and Authentication EC Enclave and Computing Environment EB Enclave Boundary Defense PE Physical and Environmental PR Personnel CO Continuity VI Vulnerability and Incident Management Answer B is incorrect. Business continuity management is an International information security standard.

NEW QUESTION: 170

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

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference:

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: C is incorrect. Configuration Management (CM) is an Information Technology Infrastructure Library (ITIL) IT Service Management (ITSM) process. It tracks all of the individual Configuration Items (CI) in an IT system, which may be as simple as a single server, or as complex as the entire IT department. In large organizations a configuration manager may be appointed to oversee and manage the CM process.

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: 171

According to the NIST SAMATE, dynamic analysis tools operate by generating runtime vulnerability scenario using some functions. Which of the following are functions that are used by the dynamic analysis tools and are summarized in the NIST SAMATE? Each correct answer represents a complete solution.

Choose all that apply.

- A. Implementation attack
- B. Source code security
- C. File corruption
- D. Network fault injection

Answer: A,C,D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: According to the NIST SAMATE, dynamic analysis tools operate by generating runtime vulnerability scenario using the following functions: Resource fault injection Network fault injection System fault injection User interface fault injection Design attack Implementation attack File corruption AnswerB is incorrect. This function is summarized for static analysis tools.

NEW QUESTION: 172

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

- A. Leverage attack patterns
- B. Compiler security checking and enforcement
- C. Tools to detect memory violations
- D. Safe software libraries
- E. Code for reuse and maintainability

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: The tools and practices that are helpful in producing secure software are summarized in the report "Enhancing the Development Life Cycle to Produce Secure Software". The tools and practices are as follows: Compiler security checking and enforcement Safe software libraries Runtime error checking and safety enforcement Tools to detect memory violations Code obfuscation AnswerA and E are incorrect. These are secure coding principles and practices of defensive coding.

NEW QUESTION: 173

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: 174

According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Which of the following are among the eight areas of IA defined by DoD? Each correct answer represents a complete solution. Choose all that apply.

A. VI Vulnerability and Incident Management

B. Information systems acquisition, development, and maintenance

C. DC Security Design & Configuration

D. EC Enclave and Computing Environment

Answer: A,C,D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Following are the various

U.S. Department of Defense information security standards: DC Security Design & Configuration
IA Identification and Authentication EC Enclave and Computing Environment EB Enclave
Boundary Defense PE Physical and Environmental PR Personnel CO Continuity VI Vulnerability
and Incident Management

Answer B is incorrect. Business continuity management is an International information security standard.

NEW QUESTION: 175

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: A ([LEAVE A REPLY](#))

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: 176

Which of the following processes will you involve to perform the active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures?

- A. Penetration testing
- B. Baselining
- C. Risk analysis
- D. Compliance checking

Answer: ([SHOW ANSWER](#))

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. Risk analysis is the science of risks and their probability and evaluation in a business or a process. It is an important factor in security enhancement and prevention in a system. Risk analysis should be performed as part of the risk management process for each project. The outcome of the risk analysis would be

the creation or review of the risk register to identify and quantify risk elements to the project and their potential impact. Answer D is incorrect. Compliance checking performs the reviews for safeguards and controls to verify whether the entity is complying with particular procedures, rules or not. It includes the inspection of operational systems to guarantee that hardware and software controls have been correctly implemented and maintained. Compliance checking covers the activities such as penetration testing and vulnerability assessments. Compliance checking must be performed by skilled persons, or by an automated software package. Answer B is incorrect. Baselining is a method for analyzing the performance of computer networks. The method is marked by comparing the current performance to a historical metric, or "baseline". For example, if a user measured the performance of a network switch over a period of time, he could use that performance figure as a comparative baseline if he made a configuration change to the switch.

NEW QUESTION: 177

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: 178

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: 179

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: 180

The DoD 8500 policy series represents the Department's information assurance strategy. Which of the following objectives are defined by the DoD 8500 series? Each correct answer represents a complete solution. Choose all that apply.

- A. Defending systems
- B. Providing IA Certification and Accreditation
- C. Providing command and control and situational awareness
- D. Protecting information

Answer: A,C,D ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: The various objectives of the DoD 8500 series are as follows: Protecting information Defending systems Providing command and control and situational awareness Making sure that the information assurance is integrated into processes Increasing security awareness throughout the DoD's workforce

NEW QUESTION: 181

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

- A. Three
- B. Seven
- C. One
- D. Four

Answer: ([SHOW ANSWER](#))

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

Valid CSSLP Dumps shared by TrainingDump.com for Helping Passing CSSLP Exam! TrainingDump.com now offer the **newest CSSLP exam dumps**, the TrainingDump.com CSSLP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CSSLP dumps with Test Engine here:

NEW QUESTION: 182

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: 183

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

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

Answer: C ([LEAVE A REPLY](#))

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

NEW QUESTION: 184

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](#))

Explanation/Reference:

Explanation: In order to accomplish the task, you should limit the number of Syslog messages or TCP connections from a specific source for a certain time period. This will prevent a denial of service (DoS) for the Syslog server and the loss of Syslog messages from other sources. Answer: D is incorrect. You can encrypt rotated log files automatically using third-party or OS mechanisms to protect data confidentiality.

Answer A is incorrect. You can use a different message format other than Syslog in order to accept data

for aggregating data from hosts that do not support Syslog. Answer: B is incorrect. You can enable the storage of log entries in both traditional Syslog files and a database for creating a database storage for logs.

NEW QUESTION: 185

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: 186

Which of the following agencies is responsible for funding the development of many technologies such as computer networking, as well as NLS?

A. DIAP

B. DTIC

C. DARPA

D. DISA

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: The Defense Advanced Research Projects Agency (DARPA) is an agency of the United States Department of Defense responsible for the development of new technology for use by the military.

DARPA has been responsible for funding the development of many technologies which have had a major effect on the world, including computer networking, as well as NLS, which was both the first hypertext system, and an important precursor to the contemporary ubiquitous graphical user interface. DARPA supplies technological options for the entire Department, and is designed to be the "technological engine" for transforming DoD. AnswerD is incorrect. The Defense Information Systems Agency is a United States Department of Defense combat support agency with the goal of providing real-time information technology (IT) and communications support to the President, Vice President, Secretary of Defense, the military Services, and the Combatant Commands.

DISA, a Combat Support Agency, engineers and provides command and control capabilities and enterprise infrastructure to continuously operate and assure a global net-centric enterprise in direct support to joint warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations. Answer: B is incorrect. The Defense Technical Information Center (DTIC) is a repository of scientific and technical documents for the United States Department of Defense. DTIC serves the DoD community as the largest central resource for DoD and government-funded scientific, technical, engineering, and business related information available today.

DTIC's documents are available to DoD personnel and defense contractors, with unclassified documents also available to the public. DTIC's aim is to serve a vital link in the transfer of information among DoD personnel, DoD contractors, and potential contractors and other U.S. Government agency personnel and their contractors. AnswerA is incorrect. The Defense-wide Information Assurance Program (DIAP) protects and supports DoD information, information systems, and information networks, which is important to the Department and the armed forces throughout the day-to-day operations, and in the time of crisis.

The DIAP uses the OSD method to plan, observe, organize, and incorporate IA activities. The role of DIAP is to act as a facilitator for program execution by the combatant commanders, Military Services, and Defense Agencies. The DIAP staff combines functional and programmatic skills for a comprehensive Defense-wide approach to IA. The DIAP's main objective is to ensure that the DoD's vital information resources are secured and protected by incorporating IA activities to get a secure net-centric GIG operation enablement and information supremacy by applying a Defense-in-Depth methodology that integrates the capabilities of people, operations, and technology to establish a multi-layer, multidimensional protection.

NEW QUESTION: 187

An assistant from the HR Department calls you to ask the Service Hours & Maintenance Slots for your ERP system. In which document will you most probably find this information?

- A. Service Level Agreement
- B. Release Policy
- C. Service Level Requirements
- D. Underpinning Contract

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: You will most probably find this information in the Service Level Agreement document.

Amongst other information, SLA contains information about the agreed Service Hours and maintenance slots for any particular Service. Service Level Agreement (frequently abbreviated as SLA) is a part of a service contract where the level of service is formally defined. In practice, the term SLA is sometimes used to refer to the contracted delivery time (of the service) or performance. Service Level Agreement (SLA) is a negotiated agreement between two parties where one is the customer and the other is the service provider. This can be a legally binding formal or informal 'contract'. Contracts between the Service Provider and other third parties are often (incorrectly) called SLAs, as the level of service has been set by the (principal) customer there can be no 'agreement' between third parties (these agreements are simply a 'contract'). Operating Level Agreements or OLA(s) however, may be used by internal groups to support SLA (s).

AnswerB is incorrect. Release Policy is a set of rules for deploying releases into the live operational

environment, defining different approaches for releases depending on their urgency and impact.

AnswerC is incorrect. The Service Level Requirements document contains the requirements for a service from the client viewpoint, defining detailed service level targets, mutual responsibilities, and other requirements specific to a certain group of customers. Answer D is incorrect.

Underpinning Contract (UC) is a contract between an IT service provider and a third party. In another way, it is an agreement between the IT organization and an external provider about the delivery of one or more services. The third party provides services that support the delivery of a service to a customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level targets in an SLA.

NEW QUESTION: 188

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](#))

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: 189

Which of the following classification levels defines the information that, if disclosed to the unauthorized parties, could be reasonably expected to cause exceptionally grave damage to the national security?

- A.** Secret information
- B.** Unclassified information
- C.** Confidential information
- D.** Top Secret information

Answer: D ([LEAVE A REPLY](#))

Top Secret information is the highest level of classification of material on a national level. Such material would cause "exceptionally grave damage" to national security if publicly available. Answer A is incorrect. Secret information is that, if disclosed to unauthorized parties, could be expected to cause serious damage to the national security, but it is not the best answer for the above question. Answer C is incorrect. Such material would cause "damage" or be "prejudicial" to national security if publicly available. Answer B is incorrect. Unclassified information, technically, is not a classification level, but is used for government documents that do not have a classification listed above. Such documents can sometimes be viewed by those without security clearance.

NEW QUESTION: 190

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: 191

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

- A. Human factors
- B. Functional requirements
- C. Performance requirements
- D. Operational scenarios
- E. Explanation:

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

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 192

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: 193

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: C ([LEAVE A REPLY](#))

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: 194

Della work as a project manager for BlueWell Inc. A threat with a dollar value of \$250,000 is expected to happen in her project and the frequency of threat occurrence per year is 0.01. What will be the annualized loss expectancy in her project?

- A. \$2,000
- B. \$2,500
- C. \$3,510
- D. \$3,500

Answer: B ([LEAVE A REPLY](#))

The annualized loss expectancy in her project will be \$2,500. Annualized loss expectancy (ALE) is the annually expected financial loss to an organization from a threat. The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as follows: $ALE = \text{Single Loss Expectancy (SLE)} * \text{Annualized Rate of Occurrence (ARO)}$ Here, it is as follows: $ALE = SLE * ARO = 250,000 * 0.01 = 2,500$ Answer D, C, and A are incorrect. These are not valid answers.

NEW QUESTION: 195

Which of the following is a name, symbol, or slogan with which a product is identified?

- A. Trademark
- B. Copyright
- C. Trade secret
- D. Patent

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: A trademark is a name, symbol, or slogan with which a product is identified. Its uniqueness makes the product noticeable among the same type of products. For example, Pentium and Athlon are brand names of the CPUs that are manufactured by Intel and AMD, respectively. The trademark law protects a company's trademark by making it illegal for other companies to use it without taking prior permission of the trademark owner. A trademark is registered so that others cannot use identical or similar marks. Answer: C is incorrect. 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: B 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: D is incorrect. A patent is a set of exclusive rights granted to anyone who invents any new and useful machine, process, composition of matter, etc. A patent enables the inventor to legally enforce his right to exclude others from using his invention.

NEW QUESTION: 196

Which of the following life cycle modeling activities establishes service relationships and message exchange paths?

- A.** Service-oriented logical design modeling
- B.** Service-oriented conceptual architecture modeling
- C.** Service-oriented discovery and analysis modeling
- D.** Service-oriented business integration modeling

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

Explanation: The service-oriented logical design modeling establishes service relationships and message exchange paths. It also addresses service visibility and crafts service logical compositions.

Valid CSSLP Dumps shared by TrainingDump.com for Helping Passing CSSLP Exam!
TrainingDump.com now offer the **newest CSSLP exam dumps**, the TrainingDump.com CSSLP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CSSLP dumps with Test Engine here:

NEW QUESTION: 197

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)

Explanation/Reference:

Explanation: 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: 198

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

- A. Component integration and test
- B. System security analysis
- C. Security requirements allocation
- D. High level software design

Answer: (SHOW ANSWER)

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

NEW QUESTION: 199

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: ([SHOW ANSWER](#))

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: 200

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: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: 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. AnswerC 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. AnswerA 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 AnswerB 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: 201

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

- A. Enabling attack
- B. Reconnaissance attack
- C. Sabotage attack
- D. Disclosure attack

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

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

NEW QUESTION: 202

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.

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: 203

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: 204

Which of the following secure coding principles and practices defines the appearance of code listing so that a code reviewer and maintainer who have not written that code can easily understand it?

- A. Make code forward and backward traceable
- B. Review code during and after coding
- C. Use a consistent coding style
- D. Keep code simple and small

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference:

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

NEW QUESTION: 205

Which of the following security related areas are used to protect the confidentiality, integrity, and availability of federal information systems and information processed by those systems?

- A. Personnel security
- B. Access control
- C. Configuration management
- D. Media protection
- E. Risk assessment

Answer: ([SHOW ANSWER](#))

The minimum security requirements cover seventeen security related areas to protect the confidentiality, integrity, and availability of federal information systems and information processed by those systems. They are as follows: Access control Awareness and training Audit and accountability Certification, accreditation, and security assessment Configuration management Contingency planning Identification and authentication Incident response Maintenance Media protection Physical and environmental protection Planning Personnel security Risk assessment Systems and services acquisition System and communications protection System and information integrity

NEW QUESTION: 206

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

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

Choose all that apply.

- A. Common controls
- B. Hybrid controls
- C. Storage controls
- D. System-specific controls

Answer: A,B,D ([LEAVE A REPLY](#))

Explanation/Reference:

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

NEW QUESTION: 207

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](#))

Explanation/Reference:

Explanation: When an agent detects a policy violation for data of all states, the Data Loss prevention (DLP) technology takes one of the following actions: It creates an alert. It notifies an administrator of a violation. It quarantines the file to a secure location. It encrypts the file. It blocks the transmission of content. Answer:

C is incorrect. Data Loss Prevention (DLP) reconstructs the session when data is in motion.

NEW QUESTION: 208

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](#))

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: 209

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.

Valid CSSLP Dumps shared by TrainingDump.com for Helping Passing CSSLP Exam!
TrainingDump.com now offer the **newest CSSLP exam dumps**, the TrainingDump.com
CSSLP exam **questions have been updated** and **answers have been corrected** get the
newest TrainingDump.com CSSLP dumps with Test Engine here:
<https://www.trainingdump.com/ISC/CSSLP-practice-exam-dumps.html> (349 Q&As Dumps,
40%OFF Special Discount: Exam-Tests)