

ISC.CSSLP.v2022-07-31.q153

Exam Code:	CSSLP
Exam Name:	Certified Secure Software Lifecycle Professional Practice Test
Certification Provider:	ISC
Free Question Number:	153
Version:	v2022-07-31
# of views:	4802
# of Questions views:	8059
https://www.dumpsfiles.com/files/ISC/CSSLP/ISC.CSSLP.v2022-07-31.q153	

NEW QUESTION: 1

A number of security patterns for Web applications under the DARPA contract have been developed by Kienzle, Elder, Tyree, and Edwards-Hewitt. Which of the following patterns are applicable to aspects of authentication in Web applications?b Each correct answer represents a complete solution. Choose all that apply.

- A. Authenticated session
- B. Secure assertion
- C. Partitioned application
- D. Password authentication
- E. Account lockout
- F. Password propagation

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation: The various patterns applicable to aspects of authentication in the Web applications are as follows: Account lockout: It implements a limit on the incorrect password attempts to protect an account from automated password-guessing attacks. Authenticated session: It allows a user to access more than one access-restricted Web page without re-authenticating every page. It also integrates user authentication into the basic session model. Password authentication: It provides protection against weak passwords, automated password-guessing attacks, and mishandling of passwords. Password propagation:

It offers a choice by requiring that a user's authentication credentials be verified by the database before providing access to that user's data. AnswerB and C are incorrect. Secure assertion and partitioned application patterns are applicable to software assurance in general.

NEW QUESTION: 2

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

- A. Port Scanning
- B. Discovery Scanning
- C. Server Scanning
- D. Workstation Scanning

Answer: ([SHOW ANSWER](#))

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

NEW QUESTION: 3

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

Explanation/Reference:

Explanation: 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. AnswerC is incorrect. The crisis communication plan can be broadly defined as the plan for the exchange of information before, during, or after a crisis event. It is considered as a sub-specialty of the public relations profession that is designed to protect and defend an individual, company, or organization facing a public challenge to its reputation. The aim of crisis communication plan is to assist organizations to achieve continuity of critical business processes and information flows under crisis, disaster or event driven circumstances. Answer: A is incorrect. A contingency plan is a plan devised for a specific situation when things could go wrong.

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

NEW QUESTION: 4

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

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

Answer: ([SHOW ANSWER](#))

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: 5

Which of the following are the principle duties performed by the BIOS during POST (power-onself-test)? Each correct answer represents a part of the solution. Choose all that apply.

- A. It provides a user interface for system's configuration.
- B. It identifies, organizes, and selects boot devices.
- C. It delegates control to other BIOS, if it is required.
- D. It discovers size and verifies system memory.
- E. It verifies the integrity of the BIOS code itself.
- F. It interrupts the execution of all running programs.

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

The principle duties performed by the BIOS during POST (power-on-self-test) are as follows: It verifies the integrity of the BIOS code itself. It discovers size and verifies system memory. It discovers, initializes, and catalogs all system hardware. It delegates control to other BIOS if it is required. It provides a user interface for system's configuration. It identifies, organizes, and selects boot devices. It executes the bootstrap program. Answer F is incorrect. The BIOS does not interrupt the execution of all running programs.

NEW QUESTION: 6

Which of the following NIST Special Publication documents provides a guideline on network security testing?

- A. NIST SP 800-42
- B. NIST SP 800-53A
- C. NIST SP 800-60
- D. NIST SP 800-53
- E. NIST SP 800-37
- F. NIST SP 800-59

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

Explanation/Reference:

Explanation: NIST SP 800-42 provides a guideline on network security testing. Answer: E, D, B, F, and C are incorrect. NIST has developed a suite of documents for conducting Certification & Accreditation (C&A).

These documents are as follows: NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems. NIST Special Publication 800-53:

This document provides a guideline for security controls for Federal Information Systems. NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System. NIST Special Publication 800-59: This document is a guideline for identifying an information system as a National Security System. NIST Special Publication

800-60: This document is a guide for mapping types of information and information systems to security objectives and risk levels.

NEW QUESTION: 7

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: 8

Which of the following statements is true about residual risks?

- A.** It is the probabilistic risk after implementing all security measures.
- B.** It can be considered as an indicator of threats coupled with vulnerability.
- C.** It is a weakness or lack of safeguard that can be exploited by a threat.
- D.** It is the probabilistic risk before implementing all security measures.

Answer: A (LEAVE A REPLY)

The residual risk is the risk or danger of an action or an event, a method or a (technical) process that still conceives these dangers even if all theoretically possible safety measures would be applied. The formula to calculate residual risk is (inherent risk) x (control risk) where inherent risk is (threats vulnerability). Answer B is incorrect. In information security, security risks are considered as an indicator of threats coupled with vulnerability. In other words, security risk is a probabilistic function of a given threat agent exercising a particular vulnerability and the impact of that risk on the organization. Security risks can be mitigated by reviewing and taking responsible actions based on possible risks. Answer C is incorrect. Vulnerability is a weakness or lack of safeguard that can be exploited by a threat, thus causing harm to the information systems or networks. It can exist in hardware , operating systems, firmware, applications, and configuration files. Vulnerability has been variously defined in the current context as follows: 1.A security weakness in a Target of Evaluation due to failures in analysis, design, implementation, or operation and such. 2.Weakness in an information system or components (e.g. system security procedures, hardware design, or internal controls that could be exploited to produce an information-related misfortune.) 3.The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the system, network, application, or protocol involved.

NEW QUESTION: 9

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: 10

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

- A. Reviewing the classification assignments at regular time intervals and making changes as the business needs change.
- B. Running regular backups and routinely testing the validity of the backup data.
- C. Delegating the responsibility of the data protection duties to a custodian.
- D. Determining what level of classification the information requires.

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

Explanation/Reference:

Explanation: 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 a custodian. An information owner can be an executive or a manager of an organization. He will be responsible for the asset of information that must be protected. AnswerB is incorrect. Running regular backups and routinely testing the validity of the backup data is the responsibility of a custodian.

NEW QUESTION: 11

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](#))

Explanation/Reference:

Explanation: 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: 12

Which of the following security design principles supports comprehensive and simple design and implementation of protection mechanisms, so that an unintended access path does not exist or can be readily identified and eliminated?

A. Least privilege

B. Economy of mechanism

C. Psychological acceptability

D. Separation of duties

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

The economy of mechanism is a security design principle, which supports simple and comprehensive design and implementation of protection mechanisms, so that an unintended access path does not exist or can be readily identified and eliminated. Answer D is incorrect. Separation of duties defines that the completion of a specific sensitivity activity or access to sensitive object depends on the satisfaction of multiple conditions. Answer C is incorrect. Psychological acceptability defines the ease of use and intuitiveness of the user interface that controls and interacts with the access control mechanisms. Answer A is incorrect. Least privilege maintains that an individual, process, or other type of entity should be given the minimum privileges and resources for the minimum period of time required to complete a task.

NEW QUESTION: 13

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)

Explanation/Reference:

Explanation: Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives. It is performed on risk that have been prioritized through the qualitative risk analysis process. AnswerA 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. AnswerC 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: 14

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

A. \$68,250

B. \$92,600

C. \$72,650

D. \$67,250

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Explanation: The Single Loss Expectancy (SLE) of this project will be \$68,250. Single Loss Expectancy is a term related to Risk Management and Risk Assessment. It can be defined as the monetary value expected from the occurrence of a risk on an asset. It is mathematically expressed as follows: Single Loss Expectancy (SLE) = Asset Value (AV) * Exposure Factor (EF) where the Exposure Factor is represented in the impact of the risk over the asset, or percentage of asset lost. As an example, if the Asset Value is reduced two thirds, the exposure factor value is .66. If the asset is completely lost, the Exposure Factor is

1.0. The result is a monetary value in the same unit as the Single Loss Expectancy is expressed. Here, it is as follows:

$SLE = \text{Asset Value} * \text{Exposure Factor}$

$= 195,000 * 0.35$

$= \$68,250$

AnswerB, C, and D are incorrect. These are not valid SLE's for this project.

NEW QUESTION: 15

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: ([SHOW ANSWER](#))

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: 16

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

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

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

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.

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 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: (SHOW ANSWER)

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

NEW QUESTION: 18

Which of the following strategies is used to minimize the effects of a disruptive event on a company, and is created to prevent interruptions to normal business activity?

- A. Continuity of Operations Plan
- B. Contingency Plan
- C. Disaster Recovery Plan
- D. Business Continuity Plan

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

BCP is a strategy to minimize the consequence of the instability and to allow for the continuation of business processes. The goal of BCP is to minimize the effects of a disruptive event on a company, and is formed to avoid interruptions to normal business activity. 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. 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: C is incorrect. 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: A is incorrect. The Continuity Of Operation Plan (COOP) refers to the preparations and institutions maintained by the United States government, providing survival of federal government operations in the case of catastrophic events. It provides procedures and capabilities to sustain an organization's essential.

COOP is the procedure documented to ensure persistent critical operations throughout any period where normal operations are unattainable.

NEW QUESTION: 19

Which of the following is a chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event?

- A. Corrective controls
- B. Audit trail
- C. Security audit
- D. Detective controls
- E. Explanation:

Audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function. Audit records typically result from activities such as transactions or communications by individual people, systems, accounts, or other entities. The process that creates audit trail should always run in a privileged mode, so it could access and supervise all actions from all users, and normal user could not stop/change it. Furthermore, for the same reason, trail file or database table with a trail should not be accessible to normal users. Answer C is incorrect. A computer security audit is a manual or systematic measurable technical assessment of a system or application. Manual assessments include interviewing staff, performing security vulnerability scans, reviewing application and operating system access controls, and analyzing physical access to the systems. Automated assessments, or CAAT's, include system generated audit reports or using software to monitor and report changes to files and settings on a system. Systems can include personal computers, servers, mainframes, network routers, and switches.

Answer: B (LEAVE A REPLY)

is incorrect. Detective controls are the audit controls that are not needed to be restricted. Any control that performs a monitoring activity can likely be defined as a Detective Control. For example, it is possible that mistakes, either intentional or unintentional, can be made. Therefore, an additional Protective control is that these companies must have their financial results audited by an independent Certified Public Accountant. The role of this accountant is to act as an auditor. In fact, any auditor acts as a Detective control. If the organization in question has not properly followed the rules, a diligent auditor should be able to detect the deficiency which indicates that some control somewhere has failed. Answer A is incorrect. Reactive or corrective controls typically work in response to a detective control,

responding in such a way as to alert or otherwise correct an unacceptable condition. Using the example of account rules, either the internal Audit Committee or the SEC itself, based on the report generated by the external auditor, will take some corrective action. In this way, they are acting as a Corrective or Reactive control.

NEW QUESTION: 20

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
- E.** 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: B,C,D,E ([LEAVE A REPLY](#))

is incorrect.

It is defined as the secondary technology.

NEW QUESTION: 21

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](#)**)**

Explanation/Reference:

Explanation: The concept of availability ensures reliable and timely access to data or resources. In other words, availability ensures that the systems are up and running when needed. The availability concept also ensures that the security services are in working order. Answer: A and D are incorrect. The concept of integrity ensures that modifications are not made to data by unauthorized personnel or processes. It also ensures that unauthorized modifications are not made to data by authorized personnel or processes.

Answer B is incorrect. Accountability determines the actions and behaviors of an individual within a system, and identifies that particular individual. Audit trails and logs support accountability.

NEW QUESTION: 22

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: 23

You work as the Senior Project manager in Dotcoiss Inc. Your company has started a software project using configuration management and has completed 70% of it. You need to ensure that the network infrastructure devices and networking standards used in this project are installed in accordance with the requirements of its detailed project design documentation. Which of the following procedures will you employ to accomplish the task?

- A. Configuration identification
- B. Configuration control
- C. Functional configuration audit
- D. Physical configuration audit

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

Explanation/Reference:

Explanation: Physical Configuration Audit (PCA) is one of the practices used in Software Configuration Management for Software Configuration Auditing. The purpose of the software PCA is to ensure that the design and reference documentation is consistent with the as-built software product. PCA checks and matches the really implemented layout with the documented layout. AnswerC is incorrect.

Functional Configuration Audit or FCA is one of the practices used in Software Configuration Management for Software Configuration Auditing. FCA occurs either at delivery or at the moment of effecting the change. A Functional Configuration Audit ensures that functional and performance attributes of a configuration item are achieved. Answer B is incorrect. Configuration control is a procedure of the Configuration management. Configuration control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them. It supports the change of the functional and physical attributes of software at various points in time, and performs systematic control of changes to the identified attributes. Answer: A is incorrect. Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/ or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined. Baselining an attribute forces formal configuration change control processes to be effected in the event that these attributes are changed.

NEW QUESTION: 24

Which of the following steps of the LeGrand Vulnerability-Oriented Risk Management method determines the necessary compliance offered by risk management practices and assessment of risk levels?

- A. Assessment, monitoring, and assurance
- B. Vulnerability management
- C. Risk assessment
- D. Adherence to security standards and policies for development and deployment

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

Explanation/Reference:

Explanation: Assessment, monitoring, and assurance determines the necessary compliance that are offered by risk management practices and assessment of risk levels.

NEW QUESTION: 25

Which of the following security controls works as the totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy?

- A. Common data security architecture (CDSA)
- B. Application program interface (API)
- C. Trusted computing base (TCB)
- D. Internet Protocol Security (IPSec)

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

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: 26

DRAG DROP

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

Select and Place:

Command	Description	
Place Here	It is the activity of recording information to a log file or database about events or occurrences.	Log Analysis
Place Here	It is the activity of manually or programmatically reviewing logged information.	Intrusion Detection
Place Here	These are the notifications that are sent to an administrator whenever a specific event occurs.	Alarm Triggers
Place Here	It is a process to detect unwanted system access by monitoring both recorded information and real time events.	Monitoring
Place Here	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.	Logging

Answer:

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

Explanation/Reference:

Explanation: Auditing encompasses a wide variety of activities as follows: Logging: It is the activity of recording information to a log file or database about events or occurrences. Log Analysis: It is a systematic form of monitoring where the logged information is analyzed in detail. It is done to find out the trends and patterns as well as abnormal, unauthorized, illegal, and policy-violating activities.

Intrusion Detection: It is a process to detect unwanted system access by monitoring both recorded information and real time events.

Alarm Triggers: These are the notifications that are sent to an administrator whenever a specific event occurs. Monitoring: It is the activity of manually or programmatically reviewing logged information.

NEW QUESTION: 27

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. Answer C is incorrect. It is not a type of intellectual property.

NEW QUESTION: 28

Which of the following is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known, but by which a business can obtain an economic advantage over its competitors?

- A. Copyright
- B. Utility model
- C. Trade secret
- D. Cookie
- E. Explanation:

A trade secret is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known. It helps a business to obtain an economic advantage over its competitors or customers. In some jurisdictions, such secrets are referred to as confidential information or classified information.

Answer: (SHOW ANSWER)

is incorrect. A copyright is a form of intellectual property, which secures to its holder the exclusive right to produce copies of his or her works of original expression, such as a literary work, movie, musical work or sound recording, painting, photograph, computer program, or industrial design, for a defined, yet extendable, period of time. It does not cover ideas or facts. Copyright laws protect intellectual property from misuse by other individuals. Answer B is incorrect. A utility model is an intellectual property right to protect inventions. Answer D is incorrect. A cookie is a small bit of text that accompanies requests and pages as they move between Web servers and browsers. It contains information that is read by a Web application, whenever a user visits a site. Cookies are stored in the memory or hard disk of client computers. A Web site stores information, such as user preferences and settings in a cookie. This information helps in providing customized services to users. There is absolutely no way a Web server can access any private information about a user or his computer through cookies, unless a user provides the information. A Web server cannot access cookies created by other Web servers.

NEW QUESTION: 29

Which of the following statements about a host-based intrusion prevention system (HIPS) are true? Each correct answer represents a complete solution. Choose two.

- A. It can detect events scattered over the network.
- B. It is a technique that allows multiple computers to share one or more IP addresses.
- C. It can handle encrypted and unencrypted traffic equally.
- D. It cannot detect events scattered over the network.

Answer: C,D (LEAVE A REPLY)

A host-based intrusion prevention system (HIPS) is an application usually employed on a single computer. It complements traditional fingerprint-based and heuristic antivirus detection methods, since it does not need continuous updates to stay ahead of new malware. When a malicious code needs to modify the system or other software residing on the machine, a HIPS system will notice some of the resulting changes and prevent the action by default or notify the user for permission. It can handle encrypted and unencrypted traffic equally and cannot detect events scattered over the network. Answer B is incorrect. Network address translation (NAT) is a technique that allows multiple computers to share one or more IP addresses. NAT is configured at the server between a private network and the Internet. It allows the computers in a private network to share a global, ISP assigned address. NAT modifies the headers of packets traversing the server. For packets outbound to the Internet, it translates the source addresses from private to public, whereas for packets inbound from the Internet, it translates the destination addresses from public to private. Answer A is incorrect. Network intrusion prevention system (NIPS) is a hardware/software platform that is designed to analyze, detect, and report on security related events. NIPS is designed to inspect traffic and based on its configuration or security policy, it can drop malicious traffic. NIPS is able to detect events scattered over the network and can react.

NEW QUESTION: 30

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: 31

Which of the following are included in Technical Controls? Each correct answer represents a complete solution. Choose all that apply.

- A. Identification and authentication methods
- B. Configuration of the infrastructure
- C. Password and resource management
- D. Implementing and maintaining access control mechanisms
- E. Security devices
- F. Conducting security-awareness training

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

Technical Controls are also known as Logical Controls. These controls include the following:

Implementing and maintaining access control mechanisms Password and resource management

Identification and authentication methods Security devices Configuration of the infrastructure Answer F is incorrect. It is a part of Administrative Controls.

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

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: 33

A Web-based credit card company had collected financial and personal details of Mark before issuing him a credit card. The company has now provided Mark's financial and personal details to another company. Which of the following Internet laws has the credit card issuing company violated?

- A. Trademark law
- B. Security law
- C. Privacy law
- D. Copyright law

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

The credit card issuing company has violated the Privacy law. According to the Internet Privacy law, a company cannot provide their customer's financial and personal details to other companies. Answer A is incorrect. Trademark laws facilitate the protection of trademarks around the world. Answer B is incorrect. There is no law such as Security law. Answer D is incorrect. The Copyright law protects original works or creations of authorship including literary, dramatic, musical, artistic, and certain other intellectual works.

NEW QUESTION: 34

Penetration testing (also called pen testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit. Which of the following areas can be exploited in a penetration test? Each correct answer represents a complete solution. Choose all that apply.

- A. Kernel flaws
- B. Information system architectures
- C. Race conditions
- D. File and directory permissions
- E. Buffer overflows
- F. Trojan horses
- G. Social engineering

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

Explanation/Reference:

Explanation: Penetration testing (also called pen testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit. Following are the areas that can be exploited in a penetration test: Kernel flaws: Kernel flaws refer to the exploitation of kernel code flaws in the operating system. Buffer overflows: Buffer overflows refer to the exploitation of a software failure to properly check for the length of input data. This overflow can cause malicious behavior on the system. Race conditions: A race condition is a situation in which an attacker can gain access to a system as a privileged user. File and directory permissions: In this area, an attacker exploits weak permissions restrictions to gain unauthorized access of documents. Trojan horses: These

are malicious programs that can exploit an information system by attaching themselves in valid programs and files. Social engineering:

In this technique, an attacker uses his social skills and persuasion to acquire valuable information that can be used to conduct an attack against a system.

NEW QUESTION: 35

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

- A. OTA provisioning
- B. Access control
- C. Key hiding
- D. Device fingerprinting

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

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

NEW QUESTION: 36

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)

The vulnerability, port, and network scanning tools are used in penetration testing. Vulnerability scanning is a process in which a Penetration Tester uses various tools to assess computers, computer systems, networks or applications for weaknesses. There are a number of types of vulnerability scanners available today, distinguished from one another by a focus on particular targets. While functionality varies between different types of vulnerability scanners, they share a common, core purpose of enumerating the vulnerabilities present in one or more targets. Vulnerability scanners are a core technology component of Vulnerability management. Port scanning is the first basic step to get the details of open ports on the target system. Port scanning is used to find a hackable server with a hole or vulnerability. A port is a medium of communication between two computers. Every service on a host is identified by a unique 16-bit number called a port. A port scanner is a piece of software designed to search a network host for open ports. This is often used by administrators to check the security of their

networks and by hackers to identify running services on a host with the view to compromising it. Port scanning is used to find the open ports, so that it is possible to search exploits related to that service and application. Network scanning is a penetration testing activity in which a penetration tester or an attacker identifies active hosts on a network, either to attack them or to perform security assessment. A penetration tester uses various tools to identify all the live or responding hosts on the network and their corresponding IP addresses. Answer C is incorrect. This option comes under vulnerability scanning.

NEW QUESTION: 37

Which of the following phases of DITSCAP includes the activities that are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle?

- A.** Phase 2, Verification
- B.** Phase 3, Validation
- C.** Phase 1, Definition
- D.** Phase 4, Post Accreditation Phase

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

Explanation/Reference:

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

NEW QUESTION: 38

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He finds that the We-are-secure server is vulnerable to attacks. As a countermeasure, he suggests that the Network Administrator should remove the IPP printing capability from the server. He is suggesting this as a countermeasure against _____.

- A.** SNMP enumeration
- B.** IIS buffer overflow
- C.** NetBIOS NULL session
- D.** DNS zone transfer

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

Removing the IPP printing capability from a server is a good countermeasure against an IIS buffer overflow attack. A Network Administrator should take the following steps to prevent a Web server from IIS buffer overflow attacks: Conduct frequent scans for server vulnerabilities. Install the upgrades of Microsoft service packs. Implement effective firewalls. Apply URLScan and IISLockdown utilities.

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

NEW QUESTION: 39

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

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

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 40

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: ([SHOW ANSWER](#))

Explanation/Reference:

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

NEW QUESTION: 41

Which of the following technologies is used by hardware manufacturers, publishers, copyright holders and individuals to impose limitations on the usage of digital content and devices?

- A. Hypervisor
- B. Grid computing
- C. Code signing
- D. Digital rights management

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

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

NEW QUESTION: 42

You work as a project manager for a company. The company has started a new security software project. The software configuration management will be used throughout the lifecycle of the project. You are tasked to modify the functional features and the basic logic of the software and then make them

compatible to the initial design of the project. Which of the following procedures of the configuration management will you follow to accomplish the task?

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

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

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.

NEW QUESTION: 43

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: 44

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 AnswerE and B are incorrect. Scalability and punctuality are not addressed by a software system's security policy.

NEW QUESTION: 45

Which of the following types of attacks occurs when an attacker successfully inserts an intermediary software or program between two communicating hosts?

- A. Denial-of-service attack
- B. Dictionary attack
- C. Man-in-the-middle attack

D. Password guessing attack

Answer: C (LEAVE A REPLY)

Explanation/Reference:

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

NEW QUESTION: 46

DRAG DROP

A number of security design patterns are developed for software assurance in general. Drag and drop the appropriate security design patterns in front of their respective descriptions.

Select and Place:

Patterns	Description
Drop Here	It limits the ability of an attacker to distinguish the internal workings of an application.
Drop Here	It splits a large and complex application into two or more simple components.
Drop Here	It distributes application-specific sanity checks throughout the system.
Drop Here	It creates a wall around the Web server to include the damage occurred in the server.

Hidden implementation

Partitioned application

Secure assertion

Server sandbox

Answer:

Patterns	Description
Hidden implementation	It limits the ability of an attacker to distinguish the internal workings of an application.
Partitioned application	It splits a large and complex application into two or more simple components.
Secure assertion	It distributes application-specific sanity checks throughout the system.
Server sandbox	It creates a wall around the Web server to include the damage occurred in the server.

Explanation/Reference:

Explanation: The various patterns applicable to software assurance in general are as follows: Hidden

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

Partitioned application: It splits a large and complex application into two or more simple components.

Secure assertion: It distributes application-specific sanity checks throughout the system. Server

sandbox: It creates a wall around the Web server to include the damage that occurs because of an undetected fault in the server or an exploited vulnerability.

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 documents were developed by NIST for conducting Certification & Accreditation (C&A)? Each correct answer represents a complete solution. Choose all that apply.

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

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

Explanation/Reference:

Explanation: NIST has developed a suite of documents for conducting Certification & Accreditation (C&A).

These documents are as follows: NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems. NIST Special Publication 800-53:

This document provides a guideline for security controls for Federal Information Systems. NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System. NIST Special Publication 800-59: This document is a guideline for identifying an information system as a National Security System. NIST Special Publication

800-60: This document is a guide for mapping types of information and information systems to security objectives and risk levels. AnswerC is incorrect. There is no such type of NIST document.

NEW QUESTION: 48

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

- A. NIST
- B. Office of Management and Budget (OMB)
- C. FIPS
- D. FISMA

Answer: B,D (LEAVE A REPLY)

Explanation/Reference:

Explanation: FISMA and Office of Management and Budget (OMB) require all general support systems and major applications to be fully certified and accredited before they are put into production. General

support systems and major applications are also referred to as information systems and are required to be reaccredited every three years. Answer A is incorrect. The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. Answer: C is incorrect. The Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States federal government for use by all 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: 49

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](#))

Explanation/Reference:

Explanation: Top Secret information is the highest level of classification of material on a national level. Such material would cause "exceptionally grave damage" to national security if publicly available.

Answer:

A is incorrect. Secret information is that, if disclosed to unauthorized parties, could be expected to cause serious damage to the national security, but it is not the best answer for the above question.

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: 50

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. Answer B, D, and A are incorrect. These are invalid options.

NEW QUESTION: 51

The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise. What are the responsibilities of a Chief Information Officer?

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

- A. Facilitating the sharing of security risk-related information among authorizing officials
- B. Preserving high-level communications and working group relationships in an organization
- C. Establishing effective continuous monitoring program for the organization
- D. Proposing the information technology needed by an enterprise to achieve its goals and then working within a budget to implement the plan

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

Explanation/Reference:

Explanation: A Chief Information Officer (CIO) plays the role of a leader. The responsibilities of a Chief Information Officer are as follows: Establishes effective continuous monitoring program for the organization. Facilitates continuous monitoring process for the organizations. Preserves high-level communications and working group relationships in an organization.

Confirms that information systems are covered by a permitted security plan and monitored throughout the System Development Life Cycle (SDLC). Manages and delegates decisions to employees in large enterprises. Proposes the information technology needed by an enterprise to achieve its goals and then works within a budget to implement the plan. Answer A is incorrect. A Risk Executive facilitates the sharing of security risk-related information among authorizing officials.

NEW QUESTION: 52

Which of the following authentication methods is used to access public areas of a Web site?

- A. Anonymous authentication
- B. Biometrics authentication

C. Mutual authentication

D. Multi-factor authentication

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

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

NEW QUESTION: 53

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: 54

Which of the following steps of the LeGrand Vulnerability-Oriented Risk Management method determines the necessary compliance offered by risk management practices and assessment of risk levels?

A. Assessment, monitoring, and assurance

B. Vulnerability management

C. Risk assessment

D. Adherence to security standards and policies for development and deployment

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

Assessment, monitoring, and assurance determines the necessary compliance that are offered by risk management practices and assessment of risk levels.

NEW QUESTION: 55

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

A. Object reuse

B. Degaussing

C. Residual

D. Data remanence

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

Data remanence refers to the data that remains even after the efforts have been made for removing or erasing the data. This event occurs because of data being left intact by an insignificant file deletion operation, by storage media reformatting, or through physical properties of the storage medium. Data remanence can make unintentional disclosure of sensitive information possible. So, it is required that the storage media is released into an uncontrolled environment. Answer C and B are incorrect. These are the made-up disasters. Answer A is incorrect. Object reuse refers to reassigning some other object of a storage media that has one or more objects.

NEW QUESTION: 56

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

A. Leverage attack patterns

B. Compiler security checking and enforcement

C. Tools to detect memory violations

D. Safe software libraries

E. Code for reuse and maintainability

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

Explanation/Reference:

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

NEW QUESTION: 57

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we-are-secure.com. You have searched all open ports of the we-are-secure server. Now, you want to perform the next information-gathering step, i.e., passive OS fingerprinting. Which of the following tools can you use to accomplish the task?

- A. Superscan
- B. NBTscan
- C. Nmap
- D. P0f

Answer: ([SHOW ANSWER](#))

According to the scenario, you have searched all open ports of the we-are-secure server. Now you want to perform the next information-gathering step, i.e., passive OS fingerprinting. For this, you will use the P0f tool to accomplish the task. P0f is a passive OS fingerprinting tool that is used to identify the operating system of a target host simply by examining captured packets even when the device is behind a packet firewall. It does not generate any additional direct or indirect network traffic. P0f can also be used to gather various information, such as firewall presence, NAT use (for policy enforcement), existence of a load balancer setup, the distance to the remote system and its uptime, etc. Answer C is incorrect. Nmap is used for active OS fingerprinting. Nmap is a free open-source utility for network exploration and security auditing. It is used to discover computers and services on a computer network, thus creating a "map" of the network. Just like many simple port scanners, Nmap is capable of discovering passive services. In addition, Nmap may be able to determine various details about the remote computers. These include operating system, device type, uptime, software product used to run a service, exact version number of that product, presence of some firewall techniques and, on a local area network, even vendor of the remote network card. Nmap runs on Linux, Microsoft Windows etc. Answer A is incorrect. SuperScan is a TCP/UDP port scanner. It also works as a ping sweeper and hostname resolver. It can ping a given range of IP addresses and resolve the host name of the remote system. The features of SuperScan are as follows: It scans any port range from a built-in list or any given range. It performs ping scans and port scans using any IP range. It modifies the port list and port descriptions using the built in editor. It connects to any discovered open port using user-specified "helper" applications. It has the transmission speed control utility. Answer B is incorrect. NBTscan is a scanner that scans IP networks for NetBIOS name information. It sends a NetBIOS status query to each address in a supplied range and lists received information in human readable form. It displays IP address, NetBIOS computer name, logged-in user name and MAC address of each responded host. NBTscan works in the same manner as nbtstat, but it operates on a range of addresses instead of just one.

NEW QUESTION: 58

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

E. Explanation:

Procedural controls include incident response processes, management oversight, security awareness, and training.

F. is incorrect. Physical controls include fences, doors, locks, and fire extinguishers.

G. is incorrect. Technical controls include user authentication (login) and logical access controls, antivirus software, and firewalls.

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

is incorrect. The

legal and regulatory, or compliance controls, include privacy laws, policies, and clauses.

NEW QUESTION: 59

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](#))

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: 60

FIPS 199 defines the three levels of potential impact on organizations. Which of the following potential impact levels shows limited adverse effects on organizational operations, organizational assets, or individuals?

A. Moderate

B. Low

C. Medium

D. High

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

The potential impact is called low if the loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Answer C is incorrect. Such a type of potential impact level does not exist Answer A is incorrect. The potential

impact is known to be moderate if the loss of confidentiality, integrity, or availability is expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Answer D is incorrect. The potential impact is called high if the loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

NEW QUESTION: 61

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.

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 methods offers a number of modeling practices and disciplines that contribute to a successful service-oriented life cycle management and modeling?

- A. Service-oriented modeling framework (SOMF)
- B. Service-oriented architecture (SOA)
- C. Sherwood Applied Business Security Architecture (SABSA)
- D. Service-oriented modeling and architecture (SOMA)

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

The service-oriented modeling framework (SOMF) has been proposed by author Michael Bell as a service-oriented modeling language for software development that employs disciplines and a holistic language to provide strategic solutions to enterprise problems. 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 B is incorrect. The service-oriented architecture (SOA) is a flexible set of design principles used during the phases of systems development and integration. 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 C is incorrect. SABSA (Sherwood Applied Business Security Architecture) is a framework and methodology for Enterprise Security Architecture and Service Management. It 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.

NEW QUESTION: 63

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

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

Answer: ([SHOW ANSWER](#))

Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The C&A process is used extensively in the U.S. Federal Government. Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. Answer D is incorrect. Information Assurance (IA) is the practice of managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. While focused dominantly on information in digital form, the full range of IA encompasses not only digital but also analog or physical form. Information assurance as a field has grown from the practice of information security, which in turn grew out of practices and procedures of computer security. Answer A is incorrect. The classic information security model is used in the practice of Information Assurance (IA) to define assurance requirements. The classic information security model, also called the CIA Triad,

addresses three attributes of information and information systems, confidentiality, integrity, and availability. This C-I-A model is extremely useful for teaching introductory and basic concepts of information security and assurance; the initials are an easy mnemonic to remember, and when properly understood, can prompt systems designers and users to address the most pressing aspects of assurance. Answer B is incorrect. The Five Pillars model is used in the practice of Information Assurance (IA) to define assurance requirements. It was promulgated by the U.S. Department of Defense (DoD) in a variety of publications, beginning with the National Information Assurance Glossary, Committee on National Security Systems Instruction CNSSI-4009. Here is the definition from that publication: "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." The Five Pillars model is sometimes criticized because authentication and non-repudiation are not attributes of information or systems; rather, they are procedures or methods useful to assure the integrity and authenticity of information, and to protect the confidentiality of the same.

NEW QUESTION: 64

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](#))

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). Answer B 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. Answer C 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: 65

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

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

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

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: 66

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

- A. Public cloud
- B. Community cloud
- C. Private cloud
- D. Hybrid cloud

Answer: (SHOW ANSWER)

Explanation/Reference:

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

NEW QUESTION: 67

In which of the following levels of exception safety are operations succeeded with full guarantee and fulfill all needs in the presence of exceptional situations?

- A. Commit or rollback semantics
- B. Minimal exception safety

- C. Failure transparency
- D. Basic exception safety

Answer: ([SHOW ANSWER](#))

Failure transparency is the best level of exception safety. In this level, operations are succeeded with full guarantee and fulfill all needs in the presence of exceptional situations. Failure transparency does not throw the exception further up even when an exception occurs. This level is also known as no throw guarantee.

NEW QUESTION: 68

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

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

- A. Qualitative risk analysis
- B. Historical information
- C. Rolling wave planning
- D. Quantitative analysis

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: Qualitative risk analysis is the best answer as it is a fast and low-cost approach to analyze the risk impact and its effect. It can promote certain risks onto risk response planning. Qualitative Risk Analysis uses the likelihood and impact of the identified risks in a fast and cost-effective manner.

Qualitative Risk Analysis establishes a basis for a focused quantitative analysis or Risk Response Plan by evaluating the precedence of risks with a concern to impact on the project's scope, cost, schedule, and quality objectives.

The qualitative risk analysis is conducted at any point in a project life cycle. The primary goal of qualitative risk analysis is to determine proportion of effect and theoretical response. The inputs to the Qualitative Risk Analysis process are: Organizational process assets Project Scope Statement Risk Management Plan Risk Register Answer: B is incorrect. Historical information can be helpful in the qualitative risk analysis, but it is not the best answer for the question as historical information is not always available (consider new projects). Answer: D is incorrect. Quantitative risk analysis is in-depth and often requires a schedule and budget for the analysis. Answer: C is incorrect. Rolling wave planning is not a valid answer for risk analysis processes.

NEW QUESTION: 69

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: 70

The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum standard process for the certification and accreditation of computer and telecommunications systems that handle U.S. national security information. Which of the following participants are required in a NIACAP security assessment? Each correct answer represents a part of the solution. Choose all that apply.

- A. Certification agent
- B. Designated Approving Authority
- C. IS program manager
- D. Information Assurance Manager
- E. User representative

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

Explanation/Reference:

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

NEW QUESTION: 71

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: 72

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: 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](#))

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

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

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

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

The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk. The subordinate tasks of the Implement and Validate Assigned IA Control phase in the DIACAP process are as follows: Execute and update IA implementation plan. Conduct validation activities. Combine validation results in the DIACAP scorecard. Answer D is incorrect. The activities related to the disposition of the system data and objects are conducted in the fifth phase of the DIACAP process. The fifth phase of the DIACAP process is known as Decommission System.

NEW QUESTION: 75

Which of the following roles is also known as the accreditor?

- A.** Data owner
- B.** Chief Risk Officer
- C.** Chief Information Officer
- D.** Designated Approving Authority

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

Designated Approving Authority (DAA) is also known as the accreditor. Answer A is incorrect. The data owner (information owner) is usually a member of management, in charge of a specific business unit, and is ultimately responsible for the protection and use of a specific subset of information. Answer B is incorrect. A Chief Risk Officer (CRO) is also known as Chief Risk Management Officer (CRMO). The Chief Risk Officer or Chief Risk Management Officer of a corporation is the executive accountable for enabling the efficient and effective governance of significant risks, and related opportunities, to a business and its various segments. Risks are commonly categorized as strategic, reputational, operational, financial, or compliance-related. CRO's are accountable to the Executive Committee and The Board for enabling the business to balance risk and reward. In more complex organizations, they are generally responsible for coordinating the organization's Enterprise Risk Management (ERM) approach. Answer C is incorrect. The Chief Information Officer (CIO), or Information Technology (IT)

director, is a job title commonly given to the most senior executive in an enterprise responsible for the information technology and computer systems that support enterprise goals. The CIO plays the role of a leader and reports to the chief executive officer, chief operations officer, or chief financial officer. In military organizations, they report to the commanding officer.

NEW QUESTION: 76

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.

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

Which of the following methods determines the principle name of the current user and returns the java.security.Principal object in the HttpServletRequest interface?

- A. getUserPrincipal()
- B. isUserInRole()
- C. getRemoteUser()
- D. getCallerPrincipal()

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

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

NEW QUESTION: 78

You work as a Security Manager for Tech Perfect Inc. You want to save all the data from the SQL injection attack, which can read sensitive data from the database and modify database data using some commands, such as Insert, Update, and Delete. Which of the following tasks will you perform? Each correct answer represents a complete solution. Choose three.

- A. Apply maximum number of database permissions.
- B. Use an encapsulated library for accessing databases.
- C. Create parameterized stored procedures.
- D. Create parameterized queries by using bound and typed parameters.

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

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. Answer A is incorrect. In order to save all the data from the SQL injection attack, you should minimize database permissions.

NEW QUESTION: 79

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: 80

Which of the following is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known, but by which a business can obtain an economic advantage over its competitors?

- A.** Copyright
- B.** Utility model
- C.** Trade secret
- D.** Cookie

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation:

A trade secret is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known. It helps a business to obtain an economic advantage over its competitors or customers. In some jurisdictions, such secrets are referred to as confidential information or classified information. AnswerA 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. AnswerB is incorrect. A utility model is an intellectual property right to protect inventions. AnswerD is incorrect. A cookie is a small bit of text that accompanies requests and pages as they move between Web servers and browsers. It contains information that is read by a Web application, whenever a user visits a site. Cookies are stored in the memory or hard disk of client computers. A Web site stores information, such as user preferences and settings in a cookie. This information helps in providing customized services to users. There is absolutely no way a Web server can access any private information about a user or his computer through cookies, unless a user provides the information. A Web server cannot access cookies created by other Web servers.

NEW QUESTION: 81

Rob is the project manager of the IDLK Project for his company. This project has a budget of \$5,600,000 and is expected to last 18 months. Rob has learned that a new law may affect how the project is allowed to proceed - even though the organization has already invested over \$750,000 in the project. What risk response is the most appropriate for this instance?

- A.** Transference
- B.** Enhance

C. Mitigation

D. Acceptance

E. Explanation:

At this point all that Rob can likely do is accepting the risk event. Because this is an external risk, there is little that Rob can do other than document the risk and share the new with management and the project stakeholders. If the law is passed then Rob can choose the most appropriate way for the project to continue. 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 B is incorrect.

Mitigation aims to lower the probability and/or impact of the risk event. Answer C is incorrect.

Transference transfers the ownership of the risk event to a third party, usually through a contractual agreement.

Answer: D,E (LEAVE A REPLY)

is incorrect. Enhance is a risk response that tries to increase the probability and/or impact of the positive risk event.

NEW QUESTION: 82

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: C (LEAVE A REPLY)

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. Answer D 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. Answer A 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: 83

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: 84

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: 85

DRAG DROP

Drop the appropriate value to complete the formula.

Single Loss Expectancy = Asset Value (\$) X Placeholder

Exposure Factor (EF) Annualized Loss Expectancy (ALE)

Annualized Rate of Occurrence (ARO)

Answer:

Single Loss Expectancy = Asset Value (\$) X Exposure Factor (EF)

Exposure Factor (EF) Annualized Loss Expectancy (ALE)

Annualized Rate of Occurrence (ARO)

Explanation:

Single Loss Expectancy = Asset Value (\$) X Exposure Factor (EF)

Exposure Factor (EF) Annualized Loss Expectancy (ALE)

Annualized Rate of Occurrence (ARO)

A Single Loss Expectancy (SLE) is the value in dollar (\$) that is assigned to a single event. The SLE can be calculated by the following formula: $SLE = \text{Asset Value (\$)} \times \text{Exposure Factor (EF)}$ The Exposure Factor (EF) represents the % of assets loss caused by a threat. The EF is required to calculate the Single Loss Expectancy (SLE). The Annualized Loss Expectancy (ALE) can be calculated by multiplying the Single Loss Expectancy (SLE) with the Annualized Rate of Occurrence (ARO). $\text{Annualized Loss Expectancy (ALE)} = \text{Single Loss Expectancy (SLE)} \times \text{Annualized Rate of Occurrence (ARO)}$ Annualized Rate of Occurrence (ARO) is a number that represents the estimated frequency in which a threat is expected to occur. It is calculated based upon the probability of the event occurring and the number of employees that could make that event occur.

NEW QUESTION: 86

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: 87

DRAG DROP

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

Select and Place:

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

Cascading

Feedback

Hookup

Answer:

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

Explanation/Reference:

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

2.Internal constructs: The internal constructs include intersection, union, and difference.

NEW QUESTION: 88

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: 89

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: ([SHOW ANSWER](#))

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: 90

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

A. User data constraint

B. Authorization constraint

C. Web resource collection

D. Accounting constraint

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

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

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

NEW QUESTION: 91

In which of the following testing methodologies do assessors use all available documentation and work under no constraints, and attempt to circumvent the security features of an information system?

- A. Full operational test
- B. Penetration test
- C. Paper test
- D. Walk-through test

Answer: (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. A paper test is the least complex test in the disaster recovery and business continuity testing approaches. In this test, the BCP/DRP plan documents are distributed to the appropriate managers and BCP/DRP team members for review, markup, and comment. This approach helps the auditor to ensure that the plan is complete and that all team members are familiar with their responsibilities within the plan. Answer D is incorrect. A walk-through test is an extension of the paper testing in the business continuity and disaster recovery process. In this testing methodology, appropriate managers and BCP/DRP team members discuss and walk through procedures of the plan. They also discuss the training needs, and clarification of critical plan elements. Answer A is incorrect. A full operational test includes all team members and participants in the disaster recovery and business continuity process. This full operation test involves the mobilization of personnel. It restores operations in the same manner as an outage or disaster would. The full operational test extends the preparedness test by including actual notification, mobilization of resources, processing of data, and utilization of backup media for restoration.

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

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: 93

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: 94

In which of the following testing methods is the test engineer equipped with the knowledge of system and designs test cases or test data based on system knowledge?

- A. Integration testing
- B. Regression testing
- C. Whitebox testing
- D. Graybox testing

Answer: D (LEAVE A REPLY)

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: 95

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

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

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

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: 96

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: ([SHOW ANSWER](#))

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

NEW QUESTION: 97

You are the project manager of the GHY project for your organization. You are about to start the qualitative risk analysis process for the project and you need to determine the roles and responsibilities for conducting risk management. Where can you find this information?

- A. Risk register
- B. Staffing management plan
- C. Risk management plan
- D. Enterprise environmental factors

Answer: ([SHOW ANSWER](#))

The risk management plan defines the roles and responsibilities for conducting risk management. A Risk management plan is a document arranged by a project manager to estimate the effectiveness, predict risks, and build response plans to mitigate them. It also consists of the risk assessment matrix. Risks are built in with any project, and project managers evaluate risks repeatedly and build plans to address them. The risk management plan consists of analysis of possible risks with both high and low impacts, and the mitigation strategies to facilitate the project and avoid being derailed through which the common problems arise. Risk management plans should be timely reviewed by the project team in order to avoid having the analysis become stale and not reflective of actual potential project risks. Most critically, risk management plans include a risk strategy for project execution. Answer A is incorrect. The risk register does not define the risk management roles and responsibilities. Answer D is incorrect. Enterprise environmental factors may define the roles that risk management officials or departments play in the project, but the best answer for all projects is the risk management plan. Answer B is incorrect. The staffing management plan does not define the risk management roles and responsibilities.

NEW QUESTION: 98

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 lockout

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

Explanation/Reference:

Explanation: 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 lockout 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: 99

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

A. Enabling attack

B. Reconnaissance attack

C. Sabotage attack

D. Disclosure attack

Answer: (SHOW ANSWER)

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: 100

Which of the following security models focuses on data confidentiality and controlled access to classified information?

A. Clark-Wilson model

B. Biba model

C. Take-Grant model

D. Bell-La Padula model

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

Explanation/Reference:

Explanation: The Bell-La Padula Model is a state machine model used for enforcing access control in government and military applications. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances

for subjects. Security labels range from the most sensitive (e.g., "Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public").

The Bell-La Padula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity. Answer B is incorrect. The Biba model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject. Answer A is incorrect. The Clark-Wilson model provides a foundation for specifying and analyzing an integrity policy for a computing system. The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. The model's enforcement and certification rules define data items and processes that provide the basis for an integrity policy. The core of the model is based on the notion of a transaction. Answer: C is incorrect. 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.

NEW QUESTION: 101

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

- A. Asset information storage and correlation
- B. Transmission confidentiality protection
- C. Incident tracking and reporting
- D. Security knowledge base
- E. Graphical user interface

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

Explanation/Reference:

Explanation: The features of SIEM products are as follows: Graphical user interface (GUI): It is used in analysis for identifying potential problems and reviewing all available data that are associated with the problems. Security knowledge base: It includes information on known vulnerabilities, log messages, and other technical data. Incident tracking and hacking: It has robust workflow features to track and report

incidents. Asset information storage and correlation: It gives higher priority to an attack that affects a vulnerable OS or a main host. Answer: B is incorrect. SIEM product does not have this feature.

NEW QUESTION: 102

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

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

Answer: D (LEAVE A REPLY)

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. Answer A is incorrect. Integrity ensures that no intentional or unintentional unauthorized modification is made to data. Answer C 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: 103

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

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

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

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

Explanation/Reference:

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

NEW QUESTION: 104

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

- A. Access
- B. Benign
- C. DoS

D. Reconnaissance

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

Explanation/Reference:

Explanation: Following are the basic categories of signatures: Informational (benign): These types of signatures trigger on normal network activity. For example: ICMP echo requests The opening or closing of TCP or UDP connections Reconnaissance: These types of signatures trigger on attacks that uncover resources and hosts that are reachable, as well as any possible vulnerabilities that they might contain. For example: Reconnaissance attacks include ping sweeps DNS queries Port scanning Access: These types of signatures trigger on access attacks, which include unauthorized access, unauthorized escalation of privileges, and access to protected or sensitive data. For example: Back Orifice A Unicode attack against the Microsoft IIS NetBus DoS: These types of signatures trigger on attacks that attempt to reduce the level of a resource or system, or to cause it to crash. For example: TCP SYN floods The Ping of Death Smurf Fraggie Trinoo Tribe Flood Network

NEW QUESTION: 105

Which of the following authentication methods is used to access public areas of a Web site?

- A. Anonymous authentication
- B. Biometrics authentication
- C. Mutual authentication
- D. Multi-factor authentication

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

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

Answer B is incorrect. Biometrics authentication uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user.

NEW QUESTION: 106

Audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function. Under which of the following controls does audit control come?

- A. Reactive controls
- B. Detective controls
- C. Protective controls
- D. Preventive controls

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: Audit trail or audit log comes under detective controls. Detective controls are the audit controls that are not needed to be restricted. Any control that performs a monitoring activity can likely be defined as a Detective Control. For example, it is possible that mistakes, either intentional or unintentional, can be made. Therefore, an additional Protective control is that these companies must have their financial results audited by an independent Certified Public Accountant. The role of this accountant is to act as an auditor. In fact, any auditor acts as a Detective control. If the organization in question has not properly followed the rules, a diligent auditor should be able to detect the deficiency which indicates that some control somewhere has failed. AnswerA is incorrect. Reactive or corrective controls typically work in response to a detective control, responding in such a way as to alert or otherwise correct an unacceptable condition. Using the example of account rules, either the internal Audit Committee or the SEC itself, based on the report generated by the external auditor, will take some corrective action. In this way, they are acting as a Corrective or Reactive control. AnswerC and D are incorrect. Protective or preventative controls serve to proactively define and possibly enforce acceptable behaviors. As an example, a set of common accounting rules are defined and must be followed by any publicly traded company. Each quarter, any particular company must publicly state its current financial standing and accounting as reflected by an application of these rules. These accounting rules and the SEC requirements serve as protective or preventative controls.

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 is designed to detect unwanted attempts at accessing, manipulating, and disabling of computer systems through the Internet?

- A. DAS
- B. IPsec
- C. IDS
- D. ACL

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

Explanation/Reference:

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

NEW QUESTION: 108

You are the project manager for a construction project. The project involves casting of a column in a very narrow space. Because of lack of space, casting it is highly dangerous. High technical skill will be required for casting that column. You decide to hire a local expert team for casting that column. Which of the following types of risk response are you following?

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

Answer: (SHOW ANSWER)

According to the question, you are hiring a local expert team for casting the column. As you have transferred your risk to a third party, this is the transference risk response that you have adopted. Transference is a strategy to mitigate negative risks or threats. In this strategy, consequences and the ownership of a risk is transferred to a third party. This strategy does not eliminate the risk but transfers responsibility of managing the risk to another party. Insurance is an example of transference. Answer C is incorrect. Mitigation is a risk response planning technique associated with threats that seeks to reduce the probability of occurrence or impact of a risk to below an acceptable threshold. Risk mitigation involves taking early action to reduce the probability and impact of a risk occurring on the project. Adopting less complex processes, conducting more tests, or choosing a more stable supplier are examples of mitigation actions. Answer A is incorrect. Avoidance involves changing the project

management plan to eliminate the threat entirely. Answer B is incorrect. Acceptance response is a part of Risk Response planning process. Acceptance response delineates that the project plan will not be changed to deal with the risk. Management may develop a contingency plan if the risk does occur. Acceptance response to a risk event is a strategy that can be used for risks that pose either threats or opportunities. Acceptance response can be of two types: Passive acceptance: It is a strategy in which no plans are made to try or avoid or mitigate the risk. Active acceptance: Such responses include developing contingency reserves to deal with risks, in case they occur. Acceptance is the only response for both threats and opportunities.

NEW QUESTION: 109

System Authorization is the risk management process. System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. What are the different phases of System Authorization Plan? Each correct answer represents a part of the solution. Choose all that apply.

- A. Post-certification
- B. Post-Authorization
- C. Authorization
- D. Pre-certification
- E. Certification

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

Explanation/Reference:

Explanation: The creation of System Authorization Plan (SAP) is mandated by System Authorization. System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. It consists of four phases: Phase 1 - Pre-certification Phase 2 - Certification Phase 3 - Authorization Phase 4 - Post-Authorization

NEW QUESTION: 110

Which of the following security models focuses on data confidentiality and controlled access to classified information?

- A. Clark-Wilson model
- B. Biba model
- C. Take-Grant model
- D. Bell-La Padula model

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

The Bell-La Padula Model is a state machine model used for enforcing access control in government and military applications. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g., "Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public"). The Bell-La Padula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity. Answer B is incorrect. The Biba model is a formal state transition system of

computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject. Answer A is incorrect. The Clark-Wilson model provides a foundation for specifying and analyzing an integrity policy for a computing system. The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. The model's enforcement and certification rules define data items and processes that provide the basis for an integrity policy. The core of the model is based on the notion of a transaction. Answer C is incorrect. 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.

NEW QUESTION: 111

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. 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: 112

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: 113

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

- A. Patent
- B. Copyright
- C. Standard
- D. Trademark

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

Common types of intellectual property include copyrights, trademarks, patents, industrial design rights, and trade secrets. A copyright is a form of intellectual property, which secures to its holder the exclusive right to produce copies of his or her works of original expression, such as a literary work, movie,

musical work or sound recording, painting, photograph, computer program, or industrial design, for a defined, yet extendable, period of time. It does not cover ideas or facts. Copyright laws protect intellectual property from misuse by other individuals. A trademark is a distinctive sign used by an individual, business organization, or other legal entity to identify that the products or services to consumers with which the trademark appears originate from a unique source, and to distinguish its products or services from those of other entities. A trademark is designated by the following symbols: : It is for an unregistered trade mark and it is used to promote or brand goods. : It is for an unregistered service mark and it is used to promote or brand services. : It is for a registered trademark. A patent is a set of exclusive rights granted by a state to an inventor or their assignee for a limited period of time in exchange for a public disclosure of an invention. Answer C is incorrect. It is not a type of intellectual property.

NEW QUESTION: 114

Security is a state of well-being of information and infrastructures in which the possibilities of successful yet undetected theft, tampering, and/or disruption of information and services are kept low or tolerable. Which of the following are the elements of security? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: (SHOW ANSWER)

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

NEW QUESTION: 115

A number of security patterns for Web applications under the DARPA contract have been developed by Kienzle, Elder, Tyree, and Edwards-Hewitt. Which of the following patterns are applicable to aspects of authentication in Web applications? Each correct answer represents a complete solution. Choose all that apply.

- A. Authenticated session
- B. Secure assertion
- C. Partitioned application
- D. Password authentication
- E. Account lockout
- F. Password propagation

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

The various patterns applicable to aspects of authentication in the Web applications are as follows: Account lockout: It implements a limit on the incorrect password attempts to protect an account from

automated password-guessing attacks. Authenticated session: It allows a user to access more than one access-restricted Web page without re-authenticating every page. It also integrates user authentication into the basic session model. Password authentication: It provides protection against weak passwords, automated password-guessing attacks, and mishandling of passwords. Password propagation: It offers a choice by requiring that a user's authentication credentials be verified by the database before providing access to that user's data. Answer B and C are incorrect. Secure assertion and partitioned application patterns are applicable to software assurance in general.

NEW QUESTION: 116

Which of the following rated systems of the Orange book has mandatory protection of the TCB?

- A.** A-rated
- B.** B-rated
- C.** D-rated
- D.** C-rated

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

Explanation/Reference:

Explanation: A B-rated system of the orange book has mandatory protection of the trusted computing base (TCB).

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

NEW QUESTION: 117

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: (SHOW ANSWER)

Explanation/Reference:

Explanation: The Phase 2 of DITSCAP C&A is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. This phase takes place between the signing of the initial version of the SSAA and the formal accreditation of the system. This phase verifies security requirements during system development. The process activities of this phase are as follows: Configuring refinement of the SSAA System development Certification analysis Assessment of the Analysis Results AnswerE is incorrect. Registration is a Phase 1 activity.

NEW QUESTION: 118

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.

AnswerC 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.

AnswerA 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. AnswerB 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: 119

Which of the following is used by attackers to record everything a person types, including usernames, passwords, and account information?

- A. Packet sniffing
- B. Keystroke logging
- C. Spoofing
- D. Wiretapping

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

Keystroke logging is used by attackers to record everything a person types, including usernames, passwords, and account information. Keystroke logging is a method of logging and recording user keystrokes. It can be performed with software or hardware devices. Keystroke logging devices can

record everything a person types using his keyboard, such as to measure employee's productivity on certain clerical tasks. These types of devices can also be used to get usernames, passwords, etc. Answer D is incorrect. Wiretapping is used to eavesdrop on voice calls. Eavesdropping is the process of listening in on private conversations. It also includes attackers listening in on network traffic. Answer C is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected. Answer A is incorrect. Packet sniffing is a process of monitoring data packets that travel across a network. The software used for packet sniffing is known as sniffers. There are many packet-sniffing programs that are available on the Internet. Some of these are unauthorized, which can be harmful for a network's security.

NEW QUESTION: 120

Which of the following sections come under the ISO/IEC 27002 standard?

- A. Security policy
- B. Asset management
- C. Financial assessment
- D. Risk assessment

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

ISO/IEC 27002 is an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC) as ISO/IEC 17799:2005. This standard contains the following twelve main sections: 1.Risk assessment: It refers to assessment of risk. 2.Security policy: It deals with the security management. 3.Organization of information security: It deals with governance of information security. 4.Asset management: It refers to inventory and classification of information assets. 5.Human resources security: It deals with security aspects for employees joining, moving and leaving an organization. 6.Physical and environmental security: It is related to protection of the computer facilities. 7.Communications and operations management: It is the management of technical security controls in systems and networks. 8.Access control: It deals with the restriction of access rights to networks, systems, applications, functions and data. 9.Information systems acquisition, development and maintenance: It refers to build security into applications. 10.Information security incident management: It refers to anticipate and respond appropriately to information security breaches. 11.Business continuity management: It deals with protecting, maintaining and recovering business-critical processes and systems. 12.Compliance: It is used for ensuring conformance with information security policies, standards, laws and regulations. Answer C is incorrect. Financial assessment does not come under the ISO/IEC 27002 standard.

NEW QUESTION: 121

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.

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

Which of the following methods can be helpful to eliminate social engineering threat? Each correct answer represents a complete solution. Choose three.

- A. Password policies
- B. Data classification
- C. Data encryption
- D. Vulnerability assessments

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

The following methods can be helpful to eliminate social engineering threat: Password policies Vulnerability assessments Data classification Password policy should specify that how the password can be shared. Company should implement periodic penetration and vulnerability assessments. These assessments usually consist of using known hacker tools and common hacker techniques to breach a

network security. Social engineering should also be used for an accurate assessment. Since social engineers use the knowledge of others to attain information, it is essential to have a data classification model in place that all employees know and follow. Data classification assigns level of sensitivity of company information. Each classification level specifies that who can view and edit data, and how it can be shared.

NEW QUESTION: 123

Audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function. Under which of the following controls does audit control come?

- A.** Reactive controls
- B.** Detective controls
- C.** Protective controls
- D.** Preventive controls

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

Audit trail or audit log comes under detective controls. Detective controls are the audit controls that are not needed to be restricted. Any control that performs a monitoring activity can likely be defined as a Detective Control. For example, it is possible that mistakes, either intentional or unintentional, can be made. Therefore, an additional Protective control is that these companies must have their financial results audited by an independent Certified Public Accountant. The role of this accountant is to act as an auditor. In fact, any auditor acts as a Detective control. If the organization in question has not properly followed the rules, a diligent auditor should be able to detect the deficiency which indicates that some control somewhere has failed. Answer A is incorrect. Reactive or corrective controls typically work in response to a detective control, responding in such a way as to alert or otherwise correct an unacceptable condition. Using the example of account rules, either the internal Audit Committee or the SEC itself, based on the report generated by the external auditor, will take some corrective action. In this way, they are acting as a Corrective or Reactive control. Answer C and D are incorrect. Protective or preventative controls serve to proactively define and possibly enforce acceptable behaviors. As an example, a set of common accounting rules are defined and must be followed by any publicly traded company. Each quarter, any particular company must publicly state its current financial standing and accounting as reflected by an application of these rules. These accounting rules and the SEC requirements serve as protective or preventative controls.

NEW QUESTION: 124

Which of the following phases of NIST SP 800-37 C&A methodology examines the residual risk for acceptability, and prepares the final security accreditation package?

- A.** Security Accreditation
- B.** Initiation
- C.** Continuous Monitoring
- D.** Security Certification

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

The various phases of NIST SP 800-37 C&A are as follows: Phase 1: Initiation- This phase includes preparation, notification and resource identification. It performs the security plan analysis, update, and acceptance. Phase 2: Security Certification- The Security certification phase evaluates the controls and documentation. Phase 3: Security Accreditation- The security accreditation phase examines the residual risk for acceptability, and prepares the final security accreditation package. Phase 4: Continuous Monitoring-This phase monitors the configuration management and control, ongoing security control verification, and status reporting and documentation.

NEW QUESTION: 125

Which of the following is the process of finding weaknesses in cryptographic algorithms and obtaining the plaintext or key from the ciphertext?

- A. Cryptographer
- B. Cryptography
- C. Kerberos
- D. Cryptanalysis
- E. Explanation:

Cryptanalysis is the process of analyzing cipher text and finding weaknesses in cryptographic algorithms. These weaknesses can be used to decipher the cipher text without knowing the secret key.

Answer C is incorrect. Kerberos is an industry standard authentication protocol used to verify user or host identity. Kerberos v5 authentication protocol is the default authentication service for Windows 2000. It is integrated into the administrative and security model, and provides secure communication between Windows 2000 Server domains and clients. Answer A is incorrect. A cryptographer is a person who is involved in cryptography.

Answer: D,E (LEAVE A REPLY)

is incorrect. Cryptography is a branch of computer science and mathematics. It is used for protecting information by encoding it into an unreadable format known as cipher text.

NEW QUESTION: 126

What project management plan is most likely to direct the quantitative risk analysis process for a project in a matrix environment?

- A. Risk analysis plan
- B. Staffing management plan
- C. Risk management plan
- D. Human resource management plan
- E. Explanation:

The risk management plan defines how risks will be identified, analyzed, responded to, and then monitored and controlled regardless of the structure of the organization.

F. is

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

G. is incorrect. The staffing management plan does define how risks will be analyzed.

Answer: C (LEAVE A REPLY)

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

NEW QUESTION: 127

In which of the following deployment models of cloud is the cloud infrastructure administered by the organizations or a third party? Each correct answer represents a complete solution. Choose two.

- A.** Private cloud
- B.** Public cloud
- C.** Hybrid cloud
- D.** Community cloud

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: In private cloud, the cloud infrastructure is operated exclusively for an organization. The private cloud infrastructure is administered by the organization or a third party, and exists on premise and off premise. In community cloud, the cloud infrastructure is shared by a number of organizations and supports a particular community. The community cloud infrastructure is administered by the organizations or a third party and exists on premise or off premise. AnswerB is incorrect. In public cloud, the cloud infrastructure is administered by an organization that sells cloud services. AnswerC is incorrect. In hybrid cloud, the cloud infrastructure is administered by both, i.e., an organization and a third party.

NEW QUESTION: 128

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: ([SHOW ANSWER](#))

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: 129

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

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

C. It ensures that internal information is consistent among all subentities and also consistent with the real- world, external situation.

D. It ensures that modifications are not made to data by unauthorized personnel or processes.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

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

NEW QUESTION: 130

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: ([SHOW ANSWER](#))

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: 131

In which type of access control do user ID and password system come under?

A. Physical

B. Technical

C. Power

D. Administrative

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: Technical access controls include IDS systems, encryption, network segmentation, and antivirus controls. AnswerD is incorrect. The policies and procedures implemented by an organization come under administrative access controls. AnswerA is incorrect. Security guards, locks on the gates,

and alarms come under physical access controls. AnswerC is incorrect. There is no such type of access control as power control.

NEW QUESTION: 132

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

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

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

Explanation/Reference:

Explanation: A penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered. It is a component of a full security audit.

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

NEW QUESTION: 133

A Web-based credit card company had collected financial and personal details of Mark before issuing him a credit card. The company has now provided Mark's financial and personal details to another company.

Which of the following Internet laws has the credit card issuing company violated?

- A. Trademark law
- B. Security law
- C. Privacy law
- D. Copyright law

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

Explanation/Reference:

Explanation: The credit card issuing company has violated the Privacy law. According to the Internet Privacy law, a company cannot provide their customer's financial and personal details to other companies.

Answer A is incorrect. Trademark laws facilitate the protection of trademarks around the world. Answer: B

is incorrect. There is no law such as Security law. Answer: D is incorrect. The Copyright law protects original works or creations of authorship including literary, dramatic, musical, artistic, and certain other intellectual works.

NEW QUESTION: 134

Which of the following concepts represent the three fundamental principles of information security? Each correct answer represents a complete solution. Choose three.

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

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

The following concepts represent the three fundamental principles of information security:

1. Confidentiality 2. Integrity 3. Availability Answer B is incorrect. Privacy, authentication, accountability, authorization and identification are also concepts related to information security, but they do not represent the fundamental principles of information security.

NEW QUESTION: 135

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

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. Answer D 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: 136

Which of the following types of attacks is targeting a Web server with multiple compromised computers that are simultaneously sending hundreds of FIN packets with spoofed IP source IP addresses?

- A.** DDoS attack
- B.** Evasion attack
- C.** Insertion attack
- D.** Dictionary attack

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: A distributed denial of service (DDoS) attack targets a Web server with multiple compromised computers that are simultaneously sending hundreds of FIN packets with spoofed IP source IP addresses.

DDoS attack occurs when multiple compromised systems flood the bandwidth or resources of a targeted system, usually one or more Web servers. These systems are compromised by attackers using a variety of methods. It is an attempt to make a computer resource unavailable to its intended users. This type of attack can cause the following to occur: Saturate network resources. Disrupt connections between two computers, thereby preventing communications between services. Disrupt services on a specific computer.

AnswerD 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. AnswerC is incorrect. In an insertion attack, an IDS accepts a packet and assumes that the host computer will also accept it. But in reality, when a host system rejects the packet, the IDS accepts the attacking string that will exploit vulnerabilities in the IDS. Such attacks can badly infect IDS signatures and IDS signature analysis. Answer: B is incorrect. 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.

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

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: 138

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

- A. Structured walk-through test
- B. Full-interruption test
- C. Parallel test
- D. Simulation test

Answer: (SHOW ANSWER)

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. 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 B is incorrect. A full-interruption test includes the operations that shut down at the primary site and are shifted to the recovery site according to the disaster recovery plan. It operates just like a parallel test. The full-interruption test is very expensive and difficult to arrange. Sometimes, it causes a major disruption of operations if the test fails. 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.

NEW QUESTION: 139

In which of the following types of tests are the disaster recovery checklists distributed to the members of disaster recovery team and asked to review the assigned checklist?

- A.** Parallel test
- B.** Simulation test
- C.** Full-interruption test
- D.** Checklist test

Answer: D (LEAVE A REPLY)

A checklist test is a test in which the disaster recovery checklists are distributed to the members of the disaster recovery team. All members are asked to review the assigned checklist. The checklist test is a simple test and it is easy to conduct this test. It allows to accomplish the following three goals: It ensures that the employees are aware of their responsibilities and they have the refreshed knowledge. It provides an individual with an opportunity to review the checklists for obsolete information and update any items that require modification during the changes in the organization. It ensures that the assigned members of disaster recovery team are still working for the organization. Answer B is incorrect. A simulation test is a method used to test the disaster recovery plans. It operates just like a structured walkthrough 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. Answer A 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 C is incorrect. A full-interruption test includes the operations that shut down at the primary site and are shifted to the recovery site according to the disaster recovery plan. It operates just like a parallel test. The full-interruption test is very expensive and difficult to arrange. Sometimes, it causes a major disruption of operations if the test fails.

NEW QUESTION: 140

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: 141

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: 142

Which of the following security controls works as the totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy?

- A. Common data security architecture (CDSA)
- B. Application program interface (API)
- C. Trusted computing base (TCB)
- D. Internet Protocol Security (IPSec)

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation: Trusted computing base (TCB) refers to hardware, software, controls, and processes that cause a computer system or network to be devoid of malicious software or hardware. Maintaining the trusted computing base (TCB) is essential for security policy to be implemented successfully. 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: 143

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: 144

You work as the senior project manager in SoftTech Inc. You are working on a software project using configuration management. Through configuration management you are decomposing the verification system into identifiable, understandable, manageable, traceable units that are known as Configuration Items (CIs). According to you, which of the following processes is known as the decomposition process of a verification system into Configuration Items?

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

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Explanation: Configuration identification is known as the decomposition process of a verification system into Configuration Items. Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined.

Baselining an attribute forces formal configuration change control processes to be effected in the event that these attributes are changed. Answer: D is incorrect. Configuration control is a procedure of the Configuration management. Configuration control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them. It supports the change of the functional and physical attributes of software at various points in time, and performs systematic control of changes to the identified attributes. Configuration control is a means of ensuring that system changes are

approved before being implemented. Only the proposed and approved changes are implemented, and the implementation is complete and accurate. Answer: A is incorrect. The configuration status accounting procedure is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time. It supports the functional and physical attributes of software at various points in time, and performs systematic control of accounting to the identified attributes for the purpose of maintaining software integrity and traceability throughout the software development life cycle.

Answer C is incorrect. Configuration auditing is the quality assurance element of configuration management. It is occupied in the process of periodic checks to establish the consistency and completeness of accounting information and to validate that all configuration management policies are being followed. Configuration audits are broken into functional and physical configuration audits. They occur either at delivery or at the moment of effecting the change. A functional configuration audit ensures that functional and performance attributes of a configuration item are achieved, while a physical configuration audit ensures that a configuration item is installed in accordance with the requirements of its detailed design documentation.

NEW QUESTION: 145

Single Loss Expectancy (SLE) represents an organization's loss from a single threat. Which of the following formulas best describes the Single Loss Expectancy (SLE)?

- A. $SLE = \text{Asset Value (AV)} * \text{Exposure Factor (EF)}$
- B. $SLE = \text{Annualized Loss Expectancy (ALE)} * \text{Annualized Rate of Occurrence (ARO)}$
- C. $SLE = \text{Annualized Loss Expectancy (ALE)} * \text{Exposure Factor (EF)}$
- D. $SLE = \text{Asset Value (AV)} * \text{Annualized Rate of Occurrence (ARO)}$

Answer: A (LEAVE A REPLY)

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: $\text{Single Loss Expectancy (SLE)} = \text{Asset Value (AV)} * \text{Exposure Factor (EF)}$ 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. Answer C, D, and B are incorrect. These are not valid formulas of SLE.

NEW QUESTION: 146

The Web resource collection is a security constraint element summarized in the Java Servlet Specification v2.4. Which of the following elements does it include? Each correct answer represents a complete solution. Choose two.

- A. HTTP methods
- B. Role names
- C. Transport guarantees
- D. URL patterns

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

Explanation/Reference:

Explanation: Web resource collection is a set of URL patterns and HTTP operations that define all resources required to be protected. It is a security constraint element summarized in the Java Servlet Specification v2.4. The Web resource collection includes the following elements: URL patterns HTTP methods Answer B is incorrect. An authorization constraint includes role names. Answer: C is incorrect. A user data constraint includes transport guarantees.

NEW QUESTION: 147

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: 148

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

- A.** It is employed in a layer that relies outside of the software code or uses attributes of the code.
- B.** It applies the security policies on the software applications at their runtime.
- C.** In this security, authentication decisions are made based on the business logic.
- D.** In this security, the security decisions are based on explicit statements.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

Explanation: Declarative security applies the security policies on the software applications at their runtime.

In this type of security, the security decisions are based on explicit statements that confine security behavior. Declarative security applies security permissions that are required for the software application to access the local resources and provides role-based access control to an individual software

component and software application. It is employed in a layer that relies outside of the software code or uses attributes of the code. Answer C is incorrect. In declarative security, authentication decisions are coarse-grained in nature from an operational or external security perspective.

NEW QUESTION: 149

Which of the following security issues does the Bell-La Padula model focus on?

- A.** Authorization
- B.** Confidentiality
- C.** Integrity
- D.** Authentication

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

Explanation/Reference:

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

NEW QUESTION: 150

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

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: 151

Which of the following models manages the software development process if the developers are limited to go back only one stage to rework?

- A. Waterfall model
- B. Spiral model
- C. RAD model
- D. Prototyping model

Answer: A (LEAVE A REPLY)

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

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

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: [\(SHOW ANSWER\)](#)

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: 153

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

- A. Security Test and Evaluation (ST&E)
- B. Penetration testing
- C. Automated vulnerability scanning tool
- D. On-site interviews

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

Explanation/Reference:

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

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)