

Exam Questions CSSLP

Certified Information Systems Security Professional

<https://www.2passeasy.com/dumps/CSSLP/>



NEW QUESTION 1

Joseph works as a Software Developer for WebTech Inc. He wants to protect the algorithms and the techniques of programming that he uses in developing an application. Which of the following laws are used to protect a part of software?

- A. Code Security law
- B. Patent laws
- C. Trademark laws
- D. Copyright laws

Answer: B

Explanation:

Patent laws are used to protect the duplication of software. Software patents cover the algorithms and techniques that are used in creating the software. It does not cover the entire program of the software. Patents give the author the right to make and sell his product. The time of the patent of a product is limited though, i.e., the author of the product has the right to use the patent for only a specific length of time. Answer D is incorrect. Copyright laws protect original works or creations of authorship including literary, dramatic, musical, artistic, and certain other intellectual works.

NEW QUESTION 2

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: ABC

Explanation:

The Organization Level is the Tier 1, and it addresses risks from an organizational perspective. It includes the following points: The techniques and methodologies an organization plans to employ, to evaluate information system-related security risks. During risk assessment, the methods and procedures the organization plans to use, to evaluate the significance of the risks identified. The types and extent of risk mitigation measures the organization plans to employ, to address identified risks. The level of risk tolerance. According to the environment of operation, how the organization plans to monitor risks on an ongoing basis, given the inevitable changes to organizational information system.

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

NEW QUESTION 3

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

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

Answer: A

Explanation:

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

NEW QUESTION 4

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

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

Answer: C

Explanation:

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

NEW QUESTION 5

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

Explanation:

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 6

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of `www.we-are-secure.com`. In order to do so, he performs the following steps of the pre-attack phase successfully: Information gathering Determination of network range Identification of active systems Location of open ports and applications Now, which of the following tasks should he perform next?

- A. Perform OS fingerprinting on the We-are-secure network.
- B. Map the network of We-are-secure Inc.
- C. Install a backdoor to log in remotely on the We-are-secure server.
- D. Fingerprint the services running on the we-are-secure network.

Answer: A

Explanation:

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

NEW QUESTION 7

Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. Which of the following statements are true about Certification and Accreditation? Each correct answer represents a complete solution. Choose two.

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

Answer: AC

Explanation:

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

NEW QUESTION 8

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

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

Answer: A

Explanation:

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

| Governance Body | Membership | Responsibilities |
|---|--|--|
| Information Security Steering 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 9

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

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

Answer: D

Explanation:

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

NEW QUESTION 10

The service-oriented modeling framework (SOMF) provides a common modeling notation to address alignment between business and IT organizations. Which of the following principles does the SOMF concentrate on? Each correct answer represents a part of the solution. Choose all that apply.

- A. Architectural components abstraction
- B. SOA value proposition
- C. Business traceability
- D. Disaster recovery planning
- E. Software assets reuse

Answer: ABCE

Explanation:

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

NEW QUESTION 10

Which of the following methods does the Java Servlet Specification v2.4 define in the HttpServletRequest interface that control programmatic security? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BCD

Explanation:

The various methods of the HttpServletRequest interface are as follows: getRemoteUser(): It returns the user name that is used for the client authentication. The value of the getRemoteUser() method returns null if no user is authenticated. isUserInRole(): It determines whether the remote user is granted a specified user role. The value of the isUserInRole() method returns true if the remote user is granted the specified user role; otherwise it returns false. getUserPrincipal(): It determines the principle name of the current user and returns the java.security.Principal object. The java.security.Principal object contains the remote user name. The value of the getUserPrincipal() method returns null if no user is authenticated. Answer A is incorrect. It is not defined in the HttpServletRequest interface. The getCallerIdentity() method is used to obtain the java.security.Identity of the caller.

NEW QUESTION 11

Which of the following DoD directives is referred to as the Defense Automation Resources Management Manual?

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

Answer: B

Explanation:

The various DoD directives are as follows:

DoD 5200.1-R: This DoD directive refers to the 'Information Security Program Regulation'. DoD 5200.22-M: This DoD directive refers the 'National Industrial Security Program Operating Manual'. DoD 7950.1-M: This DoD directive refers to the 'Defense Automation Resources Management Manual'. DoDD 8000.1: This DoD directive refers to the 'Defense Information Management (IM) Program'. DoD 8910.1: This DoD directive refers to the 'Management and Control of Information Requirements'.

NEW QUESTION 12

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

Explanation:

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

NEW QUESTION 13

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

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

Answer: C

Explanation:

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

NEW QUESTION 14

The IAM/CA makes certification accreditation recommendations to the DAA. The DAA issues accreditation determinations. Which of the following are the accreditation determinations issued by the DAA? Each correct answer represents a complete solution. Choose all that apply.

- A. IATT
- B. IATO
- C. DATO
- D. ATO
- E. ATT

Answer: ABCD

Explanation:

The DAA issues one of the following four accreditation determinations: Approval to Operate (ATO): It is an authorization of a DoD information system to process, store, or transmit information. Interim Approval to Operate (IATO): It is a temporary approval to operate based on an assessment of the implementation status of the assigned IA Controls. Interim Approval to Test (IATT): It is a temporary approval to conduct system testing based on an assessment of the implementation status of the assigned IA Controls. Denial of Approval to Operate (DATO): It is a determination that a DoD information system cannot operate because of an inadequate IA design or failure to implement assigned IA Controls. Answer E is incorrect. No such type of accreditation determination exists.

NEW QUESTION 15

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

- A. Full operational test
- B. Penetration test

- C. Paper test
- D. Walk-through test

Answer: B

Explanation:

A penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered. It is a component of a full security audit. Answer C is incorrect. A paper test is the least complex test in the disaster recovery and business continuity testing approaches. In this test, the BCP/DRP plan documents are distributed to the appropriate managers and BCP/DRP team members for review, markup, and comment. This approach helps the auditor to ensure that the plan is complete and that all team members are familiar with their responsibilities within the plan. Answer D is incorrect. A walk-through test is an extension of the paper testing in the business continuity and disaster recovery process. In this testing methodology, appropriate managers and BCP/DRP team members discuss and walk through procedures of the plan. They also discuss the training needs, and clarification of critical plan elements. Answer A is incorrect. A full operational test includes all team members and participants in the disaster recovery and business continuity process. This full operation test involves the mobilization of personnel. It restores operations in the same manner as an outage or disaster would. The full operational test extends the preparedness test by including actual notification, mobilization of resources, processing of data, and utilization of backup media for restoration.

NEW QUESTION 16

Which of the following is a variant with regard to Configuration Management?

- A. A CI that has the same name as another CI but shares no relationship.
- B. A CI that particularly refers to a software version.
- C. A CI that has the same essential functionality as another CI but a bit different in some small manner.
- D. A CI that particularly refers to a hardware specification.

Answer: C

Explanation:

A CI that has the same essential functionality as another CI but a bit different in some small manner, and therefore, might be required to be analyzed along with its generic group. A Configuration item (CI) is an IT asset or a combination of IT assets that may depend and have relationships with other IT processes. A CI will have attributes which may be hierarchical and relationships that will be assigned by the configuration manager in the CM database. The Configuration Item (CI) attributes are as follows:

- * 1.Technical: It is data that describes the CI's capabilities which include software version and model numbers, hardware and manufacturer specifications, and other technical details like networking speeds, and data storage size. Keyboards, mice and cables are considered consumables.
- * 2.Ownership: It is part of financial asset management, ownership attributes, warranty, location, and responsible person for the CI.
- * 3.Relationship: It is the relationship among hardware items, software, and users. Answer B, D, and A are incorrect. These are incorrect definitions of a variant with regard to Configuration Management.

NEW QUESTION 19

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

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

Answer: ABCDE

Explanation:

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

NEW QUESTION 20

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

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

Answer: C

Explanation:

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

NEW QUESTION 25

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

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 Fraggles Trinoo Tribe Flood Network

NEW QUESTION 28

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

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

Answer: D

Explanation:

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

NEW QUESTION 32

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

- A. Take-Grant Protection Model
- B. Biba Integrity Model
- C. Bell-LaPadula Model
- D. Access Matrix

Answer: A

Explanation:

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

NEW QUESTION 34

You work as a Network Auditor for Net Perfect Inc. The company has a Windows-based network. While auditing the company's network, you are facing problems in searching the faults and other entities that belong to it. Which of the following risks may occur due to the existence of these problems?

- A. Residual risk
- B. Secondary risk
- C. Detection risk
- D. Inherent risk

Answer: C

Explanation:

Detection risks are the risks that an auditor will not be able to find what they are looking to detect. Hence, it becomes tedious to report negative results when material conditions (faults) actually exist. Detection risk includes two types of risk: Sampling risk: This risk occurs when an auditor falsely accepts or erroneously rejects an audit sample. Nonsampling risk: This risk occurs when an auditor fails to detect a condition because of not applying the appropriate procedure or using procedures inconsistent with the audit objectives (detection faults). Answer A is incorrect. Residual risk is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible

safety measures would be applied (scientifically conceivable measures). The formula to calculate residual risk is (inherent risk) x (control risk) where inherent risk is (threats vulnerability). In the economic context, residual means "the quantity left over at the end of a process; a remainder". Answer D is incorrect. Inherent risk, in auditing, is the risk that the account or section being audited is materially misstated without considering internal controls due to error or fraud. The assessment of inherent risk depends on the professional judgment of the auditor, and it is done after assessing the business environment of the entity being audited. Answer B is incorrect. A secondary risk is a risk that arises as a straight consequence of implementing a risk response. The secondary risk is an outcome of dealing with the original risk. Secondary risks are not as rigorous or important as primary risks, but can turn out to be so if not estimated and planned properly.

NEW QUESTION 36

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

- A. Benchmarking
- B. Six Sigma
- C. ISO 9001:2000
- D. SEI-CMM

Answer: A

Explanation:

Benchmarking is the tool used by system assessment process to provide a point of reference by which performance measurements can be reviewed with respect to other organizations. Benchmarking is also recognized as Best Practice Benchmarking or Process Benchmarking. It is a process used in management and mostly useful for strategic management. It is the process of comparing the business processes and performance metrics including cost, cycle time, productivity, or quality to another that is widely considered to be an industry standard benchmark or best practice. It allows organizations to develop plans on how to implement best practice with the aim of increasing some aspect of performance. Benchmarking might be a one-time event, although it is frequently treated as a continual process in which organizations continually seek out to challenge their practices. It allows organizations to develop plans on how to make improvements or adapt specific best practices, usually with the aim of increasing some aspect of performance. Answer C is incorrect. The ISO 9001:2000 standard combines the three standards 9001, 9002, and 9003 into one, called 9001. Design and development procedures are required only if a company does in fact engage in the creation of new products. The 2000 version sought to make a radical change in thinking by actually placing the concept of process management front and center ("Process management" was the monitoring and optimizing of a company's tasks and activities, instead of just inspecting the final product). The ISO 9001:2000 version also demands involvement by upper executives, in order to integrate quality into the business system and avoid delegation of quality functions to junior administrators. Another goal is to improve effectiveness via process performance metrics numerical measurement of the effectiveness of tasks and activities. Expectations of continual process improvement and tracking customer satisfaction were made explicit. Answer B is incorrect. Six Sigma is a business management strategy, initially implemented by Motorola. As of 2009 it enjoys widespread application in many sectors of industry, although its application is not without controversy. Six Sigma seeks to improve the quality of process outputs by identifying and removing the causes of defects and variability in manufacturing and business processes. It uses a set of quality management methods, including statistical methods, and creates a special infrastructure of people within the organization ("Black Belts", "Green Belts", etc.) who are experts in these methods. Each Six Sigma project carried out within an organization follows a defined sequence of steps and has quantified financial targets (cost reduction or profit increase). The often used Six Sigma symbol is as follows:



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

NEW QUESTION 40

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

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 45

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

Explanation:

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 48

Della works as a security engineer for BlueWell Inc. She wants to establish configuration management and control procedures that will document proposed or actual changes to the information system. Which of the following phases of NIST SP 800-37 C&A methodology will define the above task?

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

Answer: C

Explanation:

The various phases of NIST SP 800-37 C&A are as follows:

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

NEW QUESTION 52

Which of the following tools is used to attack the Digital Watermarking?

- A. Steg-Only Attack
- B. Active Attacks
- C. 2Mosaic
- D. Gifshuffle

Answer: C

Explanation:

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

NEW QUESTION 54

Which of the following actions does the Data Loss Prevention (DLP) technology take when an agent detects a policy violation for data of all states? Each correct answer represents a complete solution. Choose all that apply.

- A. It creates an alert.
- B. It quarantines the file to a secure location.
- C. It reconstructs the session.
- D. It blocks the transmission of content.

Answer: ABD

Explanation:

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

NEW QUESTION 58

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

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 60

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

Explanation:

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

NEW QUESTION 65

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

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

Answer: D

Explanation:

The data owner is responsible for ensuring that the appropriate security controls are in place, for assigning the initial classification to the data to be protected, for approving access requests from other parts of the organization, and for periodically reviewing the data classifications and access rights. Data owners are primarily responsible for determining the data's sensitivity or classification levels, whereas the data custodian has the responsibility for backup, retention, and recovery of data. The data owner delegates these responsibilities to the custodian. Answer B, A, and C are incorrect. These are not the valid answers.

NEW QUESTION 69

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: ACDEFG

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 70

The Project Risk Management knowledge area focuses on which of the following processes? Each correct answer represents a complete solution. Choose all that apply.

- A. Risk Monitoring and Control
- B. Risk Management Planning
- C. Quantitative Risk Analysis
- D. Potential Risk Monitoring

Answer: ABC

Explanation:

The Project Risk Management knowledge area focuses on the following processes: Risk Management Planning Risk Identification Qualitative Risk Analysis Quantitative Risk Analysis Risk Response Planning Risk Monitoring and Control Answer D is incorrect. There is no such process in the Project Risk Management knowledge area.

NEW QUESTION 73

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

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

Answer: ACD

Explanation:

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

NEW QUESTION 74

Fred is the project manager of the CPS project. He is working with his project team to prioritize the identified risks within the CPS project. He and the team are prioritizing risks for further analysis or action by assessing and combining the risks probability of occurrence and impact. What process is Fred completing?

- A. Risk identification
- B. Risk Breakdown Structure creation
- C. Perform qualitative analysis
- D. Perform quantitative analysis

Answer: C

Explanation:

Qualitative ranks the probability and impact and then helps the project manager and team to determine which risks need further analysis. Perform Qualitative Risk Analysis is the process of prioritizing risks for further analysis and action. It combines risks and their probability of occurrences and ranks them accordingly. It enables organizations to improve the project's performance by focusing on high-priority risks. Perform Qualitative Risk Analysis is usually a rapid and cost-effective means of establishing priorities for Plan Risk Responses. It also lays the foundation for Perform Quantitative Risk Analysis. Answer A is incorrect. Risk identification precedes this activity. Answer B is incorrect. This process does not describe the decomposition and organization of risks that you will complete in a risk breakdown structure. Answer D is incorrect. Quantitative analysis is the final step of risk analysis. Note the question tells you that Fred and the team will identify risks for additional analysis.

NEW QUESTION 76

The build environment of secure coding consists of some tools that actively support secure specification, design, and implementation. Which of the following features do these tools have? Each correct answer represents a complete solution. Choose all that apply.

- A. They decrease the exploitable flaws and weaknesses.
- B. They reduce and restrain the propagation, extent, and damage that have occurred by insecure software behavior.
- C. They decrease the attack surface.
- D. They employ software security constraints, protections, and service
- E. They decrease the level of type checking and program analysis.

Answer: ABCD

Explanation:

The tools that produce secure software have the following features: They decrease the exploitable flaws and weaknesses. They decrease the attack surface. They employ software security constraints, protections, and services. They reduce and restrain the propagation, extent, and damage that are caused by the behavior of insecure software. Answer E is incorrect. This feature is not required for these tools.

NEW QUESTION 79

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

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

Answer: C

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. Answer D is incorrect. The human resources management plan does define how risks will be analyzed. Answer B is incorrect. The staffing management plan does define how risks will be analyzed. Answer A is incorrect. The risk analysis plan does define how risks will be analyzed.

NEW QUESTION 84

Which of the following techniques is used when a system performs the penetration testing with the objective of accessing unauthorized information residing inside a computer?

- A. Biometrician
- B. Van Eck Phreaking
- C. Port scanning
- D. Phreaking

Answer: C

Explanation:

Port scanning identifies open doors to a computer. Hackers and crackers use this technique to obtain unauthorized information. Port scanning is the first basic step to get the details of open ports on the target system. Port scanning is used to find a hackable server with a hole or vulnerability. A port is a medium of communication between two computers. Every service on a host is identified by a unique 16-bit number called a port. A port scanner is a piece of software designed to search a network host for open ports. This is often used by administrators to check the security of their networks and by hackers to identify running services on a host with the view to compromising it. Port scanning is used to find the open ports, so that it is possible to search exploits related to that service and application. Answer D is incorrect. Phreaking is a process used to crack the phone system. The main aim of phreaking is to avoid paying for long-distance calls. As telephone networks have become computerized, phreaking has become closely linked with computer hacking. This is sometimes called the H/P

culture (with H standing for Hacking and P standing for Phreaking). Answer A is incorrect. It is defined as a system using a physical attribute for authenticating. Only authorized users are provided access to network or application. Answer B is incorrect. It is described as a form of eavesdropping in which special equipments are used to pick up the telecommunication signals or data within a computer device.

NEW QUESTION 86

Which of the following processes provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and the security posture of a system or site?

- A. NSA-IAM
- B. NIACAP
- C. ASSET
- D. DITSCAP

Answer: B

Explanation:

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

NEW QUESTION 91

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

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

Answer: B

Explanation:

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

NEW QUESTION 93

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

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

Answer: B

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 94

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

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

Answer: ABEF

Explanation:

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

collects, stores, transmits, or processes unclassified or classified information since December 1997. It identifies four phases: * 1.System Definition 2.Verification 3.Validation 4.Re-Accreditation

NEW QUESTION 96

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

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

Answer: C

Explanation:

Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The C&A process is used extensively in the U.S. Federal Government. Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. 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 97

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

- A. Unit testing
- B. Integration testing
- C. Acceptance testing
- D. Regression testing

Answer: D

Explanation:

Regression testing focuses on finding defects after a major code change has occurred. Specifically, it seeks to uncover software regressions, or old bugs that have come back. Such regressions occur whenever software functionality that was previously working correctly stops working as intended. Typically, regressions occur as an unintended consequence of program changes, when the newly developed part of the software collides with the previously existing code. Regression testing tests the system efficiency by systematically selecting the suitable and minimum set of tests that are required to effectively cover the affected changes. Answer A is incorrect. Unit testing is a type of testing in which each independent unit of an application is tested separately. During unit testing, a developer takes the smallest unit of an application, isolates it from the rest of the application code, and tests it to determine whether it works as expected. Unit testing is performed before integrating these independent units into modules. The most common approach to unit testing requires drivers and stubs to be written. Drivers and stubs are programs. A driver simulates a calling unit, and a stub simulates a called unit. Answer C is incorrect. Acceptance testing is performed on the application before its implementation into the production environment. It is done either by a client or an application specialist to ensure that the software meets the requirement for which it was made. Answer B is incorrect. Integration testing is a software testing that seeks to verify the interfaces between components against a software design. Software components may be integrated in an iterative way or all together ("big bang"). Normally the former is considered a better practice since it allows interface issues to be localized more quickly and fixed. Integration testing works to expose defects in the interfaces and interaction between the integrated components (modules). Progressively larger groups of tested software components corresponding to elements of the architectural design are integrated and tested until the software works as a system.

NEW QUESTION 100

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: A

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. Answer D 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 C 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.

NEW QUESTION 104

What are the various phases of the Software Assurance Acquisition process according to the U.S. Department of Defense (DoD) and Department of Homeland Security (DHS) Acquisition and Outsourcing Working Group?

- A. Implementing, contracting, auditing, monitoring
- B. Requirements, planning, monitoring, auditing
- C. Planning, contracting, monitoring and acceptance, follow-on
- D. Designing, implementing, contracting, monitoring

Answer: C

Explanation:

Software Assurance Acquisition process defines the level of confidence that software is free from vulnerabilities. It is designed into the software or accidentally inserted at anytime during its lifecycle, and the software works in a planned manner. According to the U.S. Department of Defense and Department of Homeland Security Acquisition and Outsourcing Working Group, the Software Assurance Acquisition process contains the following phases:

* 1.Planning 2.Contracting 3.Monitoring and acceptance 4.Follow-on

NEW QUESTION 107

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

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

Answer: B

Explanation:

Regression testing can be performed any time when a program needs to be modified either to add a feature or to fix an error. It is a process of repeating Unit testing and Integration testing whenever existing tests need to be performed again along with the new tests. Regression testing is performed to ensure that no existing errors reappear, and no new errors are introduced. Answer D is incorrect. The acceptance testing is performed on the application before its implementation into the production environment. It is done either by a client or an application specialist to ensure that the software meets the requirement for which it was made. Answer A is incorrect. Integration testing is a logical extension of unit testing. It is performed to identify the problems that occur when two or more units are combined into a component. During integration testing, a developer combines two units that have already been tested into a component, and tests the interface between the two units. Although integration testing can be performed in various ways, the following three approaches are generally used: The top-down approach The bottom-up approach The umbrella approach Answer B is incorrect. Unit testing is a type of testing in which each independent unit of an application is tested separately. During unit testing, a developer takes the smallest unit of an application, isolates it from the rest of the application code, and tests it to determine whether it works as expected. Unit testing is performed before integrating these independent units into modules. The most common approach to unit testing requires drivers and stubs to be written. Drivers and stubs are programs. A driver simulates a calling unit, and a stub simulates a called unit.

NEW QUESTION 109

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

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

Answer: D

Explanation:

Mandatory Access Control (MAC) is a model that uses a predefined set of access privileges for an object of the system. Access to an object is restricted on the basis of the sensitivity of the object and granted through authorization. Sensitivity of an object is defined by the label assigned to it. For example, if a user receives a copy of an object that is marked as "secret", he cannot grant permission to other users to see this object unless they have the appropriate permission. Answer B is incorrect. DAC is an access control model. In this model, the data owner has the right to decide who can access the data. Answer A is incorrect. Role-based access control (RBAC) is an access control model. In this model, a user can access resources according to his role in the organization. For example, a backup administrator is responsible for taking backups of important data. Therefore, he is only authorized to access this data for backing it up. However, sometimes users with different roles need to access the same resources. This situation can also be handled using the RBAC model. Answer B is incorrect. There is no such access control model as Policy Access Control.

NEW QUESTION 112

Which of the following specifies access privileges to a collection of resources by using the URL mapping?

- A. Code Access Security
- B. Security constraint
- C. Configuration Management
- D. Access Management

Answer: B

Explanation:

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

NEW QUESTION 113

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: AD

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 B is incorrect. A user data constraint includes transport guarantees.

NEW QUESTION 114

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

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

Answer: D

Explanation:

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

NEW QUESTION 119

Which of the following are the primary functions of configuration management? Each correct answer represents a complete solution. Choose all that apply.

- A. It removes the risk event entirely by adding additional steps to avoid the event.
- B. It ensures that the change is implemented in a sequential manner through formalized testing.
- C. It reduces the negative impact that the change might have had on the computing services and resources.
- D. It analyzes the effect of the change that is implemented on the system.

Answer: BCD

Explanation:

The primary functions of configuration management are as follows: It ensures that the change is implemented in a sequential manner through formalized testing. It ensures that the user base is informed of the future change. It analyzes the effect of the change that is implemented on the system. It reduces the negative impact that the change might have had on the computing services and resources. Answer A is incorrect. It is not one of the primary functions of configuration management. It is the function of risk avoidance.

NEW QUESTION 120

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

Answer: D

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 B 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 B 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 125

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: ABD

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 B is incorrect. In declarative security, authentication decisions are coarse-grained in nature from an operational or external security perspective.

NEW QUESTION 126

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

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 B is incorrect. You can use the backup control to perform back up of software and data.

NEW QUESTION 128

Which of the following statements about the authentication concept of information security management is true?

- A. It establishes the users' identity and ensures that the users are who they say they are.
- B. It ensures the reliable and timely access to resources.
- C. It determines the actions and behaviors of a single individual within a system, and identifies that particular individual.
- D. It ensures that modifications are not made to data by unauthorized personnel or processes.

Answer: A

Explanation:

The concept of authentication establishes the users' identity and ensures that the users are who they say they are. Answer B is incorrect. The concept of availability ensures the reliable and timely access to data or resources. Answer D is incorrect. The concept of integrity ensures that modifications are not made to data by unauthorized personnel or processes. Answer B is incorrect. The concept of accountability determines the actions and behaviors of a single individual within a system, and identifies that particular individual.

NEW QUESTION 132

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

- A. Change and Configuration Control
- B. Security Certification and Accreditation (C&A)
- C. Vulnerability Assessment and Penetration Testing
- D. Risk Adjustments

Answer: BCD

Explanation:

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

NEW QUESTION 135

Which of the following security models characterizes the rights of each subject with respect to every object in the computer system?

- A. Clark-Wilson model
- B. Bell-LaPadula model
- C. Biba model
- D. Access matrix

Answer: D

Explanation:

The access matrix or access control matrix is an abstract, formal security model of protection state in computer systems that characterizes the rights of each subject with respect to every object in the system. It was first introduced by Butler W. Lampson in 1971. According to the access matrix model, the protection state of a computer system can be abstracted as a set of objects 'O', that is the set of entities that needs to be protected (e.g. processes, files, memory pages) and a set of subjects 'S' that consists of all active entities (e.g. users, processes). Further there exists a set of rights 'R' of the form $r(s,o)$, where $s \in S$, $o \in O$ and $r(s,o) \in R$. A right thereby specifies the kind of access a subject is allowed to process with regard to an object. Answer B is incorrect. The Bell-La Padula Model is a state machine model used for enforcing access control in government and military applications. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g., "Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public"). The Bell-La Padula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity. 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 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.

NEW QUESTION 136

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: BD

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

NEW QUESTION 137

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

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

Answer: A

Explanation:

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

NEW QUESTION 142

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: AD

Explanation:

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 B is incorrect. Simplify the design principle is included in the General Principle 3.

NEW QUESTION 143

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

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

Answer: B

Explanation:

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

NEW QUESTION 145

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

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

Answer: B

Explanation:

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

NEW QUESTION 147

Which of the following persons in an organization is responsible for rejecting or accepting the residual risk for a system?

- A. Information Systems Security Officer (ISSO)
- B. Designated Approving Authority (DAA)
- C. System Owner
- D. Chief Information Security Officer (CISO)

Answer: B

Explanation:

The authorizing official is the senior manager responsible for approving the working of the information system. He is responsible for the risks of operating the information system within a known environment through the security accreditation phase. In many organizations, the authorizing official is also referred as approving/accrediting authority (DAA) or the Principal Approving Authority (PAA). Answer B is incorrect. The system owner has the responsibility of informing the key officials within the organization of the requirements for a security C&A of the information system. He makes the resources available, and provides the relevant documents to support the process. Answer A is incorrect. An Information System Security Officer (ISSO) plays the role of a supporter. The responsibilities of an Information System Security Officer (ISSO) are as follows: Manages the security of the information system that is slated for Certification & Accreditation (C&A). Insures the information systems configuration with the agency's information security policy. Supports the information system owner/information owner for the completion of security- related responsibilities. Takes part in the formal configuration management process. Prepares Certification & Accreditation (C&A) packages. Answer D is incorrect. The CISO has the responsibility of carrying out the CIO's FISMA responsibilities. He manages the information security program functions.

NEW QUESTION 152

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: ABD

Explanation:

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 B is incorrect. Financial assessment does not come under the ISO/IEC 27002 standard.

NEW QUESTION 155

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

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

Answer: C

Explanation:

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

NEW QUESTION 159

You work as a security engineer for BlueWell Inc. According to you, which of the following DITSCAP/NIACAP model phases occurs at the initiation of the project, or at the initial C&A effort of a legacy system?

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

Answer: B

Explanation:

The definition phase of the DITSCAP/NIACAP model takes place at the beginning of the project, or at the initial C&A effort of a legacy system. C&A consists of four phases in a DITSCAP assessment. These phases are the same as NIACAP phases. The order of these phases is as follows:

* 1.Definition: The definition phase is focused on understanding the IS business case, the mission, environment, and architecture. This phase determines the security requirements and level of effort necessary to achieve Certification & Accreditation (C&A). 2.Verification: The second phase confirms the evolving or modified system's compliance with the information. The verification phase ensures that the fully integrated system will be ready for certification testing. 3.Validation: The third phase confirms abidance of the fully integrated system with the security policy. This phase follows the requirements slated in the SSAA. The objective of the validation phase is to show the required evidence to support the DAA in accreditation process. 4.Post Accreditation: The Post Accreditation is the final phase of DITSCAP assessment and it starts after the system has been certified and accredited for operations. This phase ensures secure system management, operation, and maintenance to save an acceptable level of residual risk.

NEW QUESTION 161

Continuous Monitoring is the fourth phase of the security certification and accreditation process. What activities are performed in the Continuous Monitoring process? Each correct answer represents a complete solution. Choose all that apply.

- A. Security accreditation decision
- B. Security control monitoring and impact analyses of changes to the information system
- C. Security accreditation documentation
- D. Configuration management and control
- E. Status reporting and documentation

Answer: BDE

Explanation:

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

NEW QUESTION 165

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

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

Answer: ABD

Explanation:

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

NEW QUESTION 167

DRAG DROP

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The various DoD policy series are as follows:

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

NEW QUESTION 172

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

- A. Data classification

Answer: A

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 175

Which of the following are examples of passive attacks? Each correct answer represents a complete solution. Choose all that apply.

- A. Dumpster diving
- B. Placing a backdoor
- C. Eavesdropping
- D. Shoulder surfing

Answer: ACD

Explanation:

In eavesdropping, dumpster diving, and shoulder surfing, the attacker violates the confidentiality of a system without affecting its state. Hence, they are considered passive attacks.

NEW QUESTION 176

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.

| 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 |

- A. Mastered
 B. Not Mastered

Answer: A

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 178

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

- A. Commit or rollback semantics
 B. Minimal exception safety
 C. Failure transparency
 D. Basic exception safety

Answer: C

Explanation:

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

NEW QUESTION 182

"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: BCD

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 185

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

Explanation:

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-in-stages, 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 B is incorrect. Rapid Application Development (RAD) refers to a type of software development methodology that uses minimal planning in favor of rapid prototyping.

NEW QUESTION 186

The service-oriented modeling framework (SOMF) introduces five major life cycle modeling activities that drive a service evolution during design-time and run-time. Which of the following activities integrates SOA software assets and establishes SOA logical environment dependencies?

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

Answer: C

Explanation:

The service-oriented logical architecture modeling integrates SOA software assets and establishes SOA logical environment dependencies. It also offers foster service reuse, loose coupling and consolidation. Answer A is incorrect. The service-oriented discovery and analysis modeling discovers and analyzes services for granularity, reusability, interoperability, loose-coupling, and identifies consolidation opportunities. Answer B is incorrect. The service-oriented business integration modeling identifies service integration and alignment opportunities with business domains' processes. Answer D is incorrect. The service-oriented logical design modeling establishes service relationships and message exchange paths.

NEW QUESTION 190

How can you calculate the Annualized Loss Expectancy (ALE) that may occur due to a threat?

- A. Single Loss Expectancy (SLE) X Annualized Rate of Occurrence (ARO)
- B. Single Loss Expectancy (SLE)/ Exposure Factor (EF)
- C. Asset Value X Exposure Factor (EF)
- D. Exposure Factor (EF)/Single Loss Expectancy (SLE)

Answer: A

Explanation:

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

NEW QUESTION 195

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

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. Answer B 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 196

Which of the following ISO standards is entitled as "Information technology - Security techniques - Information security management - Measurement"?

- A. ISO 27003
- B. ISO 27005
- C. ISO 27004
- D. ISO 27006

Answer: C

Explanation:

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

NEW QUESTION 197

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: ABD

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 Answer B is incorrect. System classification is not one of the objectives of a security program.

NEW QUESTION 202

Which of the following is NOT a responsibility of a data owner?

- A. Approving access requests
- B. Ensuring that the necessary security controls are in place
- C. Delegating responsibility of the day-to-day maintenance of the data protection mechanisms to the data custodian
- D. Maintaining and protecting data

Answer: D

Explanation:

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

NEW QUESTION 207

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 210

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: ACD

Explanation:

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 212

An authentication method uses smart cards as well as usernames and passwords for authentication. Which of the following authentication methods is being referred to?

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

Answer: C

Explanation:

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

NEW QUESTION 214

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

| Code review check | Function |
|-------------------|---|
| Drop Here | It is used to check the unvalidated sources of input from URL parameters in javax.servlet.HttpServletRequest class. |
| Drop Here | It is used to check the unvalidated sources of input from Form fields in javax.servlet.HttpServletRequest class. |
| Drop Here | It is used to check the unvalidated sources of input from Cookies javax.servlet.HttpServletRequest class. |
| Drop Here | It is used to check the unvalidated sources of input from HTTP headers javax.servlet.HttpServletRequest class. |

getParameter()

getQueryString()

getCookies()

getHeaders()

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 219

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

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

Answer: D

Explanation:

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

NEW QUESTION 224

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: BCD

Explanation:

The methods of mitigating SQL injection attacks are as follows: 1.Create parameterized queries by using bound and typed parameters. 2.Create parameterized stored procedures. 3.Use a encapsulated library in order to access databases. 4.Minimize database permissions. Answer A is incorrect. In order to save all the data from the SQL injection attack, you should minimize database permissions.

NEW QUESTION 228

A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. What are the different types of policies? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ACD

Explanation:

Following are the different types of policies: Regulatory: This type of policy ensures that the organization is following standards set by specific industry regulations. This policy type is very detailed and specific to a type of industry. This is used in financial institutions, health care facilities, public utilities, and other government-regulated industries, e.g., TRAI. Advisory: This type of policy strongly advises employees regarding which types of behaviors and activities should and should not take place within the organization. It also outlines possible ramifications if employees do not comply with the established behaviors and activities. This policy type can be used, for example, to describe how to handle medical information, handle financial transactions, or process confidential information. Informative: This type of policy informs employees of certain topics. It is not an enforceable policy, but rather one to teach individuals about specific issues relevant to the company. It could explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations. Answer B is incorrect. No such type of policy exists.

NEW QUESTION 231

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CSSLP Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CSSLP Product From:

<https://www.2passeasy.com/dumps/CSSLP/>

Money Back Guarantee

CSSLP Practice Exam Features:

- * CSSLP Questions and Answers Updated Frequently
- * CSSLP Practice Questions Verified by Expert Senior Certified Staff
- * CSSLP Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CSSLP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year