

ISC2

Exam Questions CSSLP

Certified Information Systems Security Professional



NEW QUESTION 1

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

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

Answer: B

Explanation:

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

NEW QUESTION 2

Which of the following statements is true about residual risks?

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

Answer: A

Explanation:

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

NEW QUESTION 3

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

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

Answer: BCDE

Explanation:

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

NEW QUESTION 4

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 5

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

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

Answer: D

Explanation:

A checklist test is a test in which the disaster recovery checklists are distributed to the members of the disaster recovery team. All members are asked to review the assigned checklist. The checklist test is a simple test and it is easy to conduct this test. It allows to accomplish the following three goals: It ensures that the employees are aware of their responsibilities and they have the refreshed knowledge. It provides an individual with an opportunity to review the checklists for obsolete information and update any items that require modification during the changes in the organization. It ensures that the assigned members of disaster recovery team are still working for the organization. Answer B is incorrect. A simulation test is a method used to test the disaster recovery plans. It operates just like a structured walk-through test. In the simulation test, the members of a disaster recovery team present with a disaster scenario and then, discuss on appropriate responses. These suggested responses are measured and some of them are taken by the team. The range of the simulation test should be defined carefully for avoiding excessive disruption of normal business activities. Answer A is incorrect. A parallel test includes the next level in the testing procedure, and relocates the employees to an alternate recovery site and implements site activation procedures. These employees present with their disaster recovery responsibilities as they would for an actual disaster. The disaster recovery sites have full responsibilities to conduct the day-to-day organization's business. Answer C is incorrect. A full-interruption test includes the operations that shut down at the primary site and are shifted to the recovery site according to the disaster recovery plan. It operates just like a parallel test. The full-interruption test is very expensive and difficult to arrange. Sometimes, it causes a major disruption of operations if the test fails.

NEW QUESTION 6

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

- A. Compliance control
- B. Physical control
- C. Procedural control
- D. Technical control

Answer: C

Explanation:

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

NEW QUESTION 7

You work as a project manager for BlueWell Inc. You are working on a project and the management wants a rapid and cost-effective means for establishing priorities for planning risk responses in your project. Which risk management process can satisfy management's objective for your project?

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

Answer: A

Explanation:

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

NEW QUESTION 8

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

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

Answer: C

Explanation:

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

NEW QUESTION 9

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

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

Answer: 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 10

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

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

Answer: C

Explanation:

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

NEW QUESTION 10

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

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

Answer: ABCE

Explanation:

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

NEW QUESTION 15

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

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

Answer: A

Explanation:

NIST SP 800-42 provides a guideline on network security testing. Answer E, D, B, F, and C are incorrect. NIST has developed a suite of documents for conducting Certification & Accreditation (C&A). These documents are as follows: NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems. NIST Special Publication 800-53: This document provides a guideline for security controls for Federal Information Systems. NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System. NIST Special Publication 800-59: This document is a guideline for identifying an information system as a National Security System. NIST Special Publication 800-60: This document is a guide for mapping types of information and information systems to security objectives and risk levels.

NEW QUESTION 16

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 17

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 20

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

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

Answer: CDEFG

Explanation:

The potential security disadvantages of virtualization are as follows: It increases configuration effort because of complexity and composite system. It initiates the problem of how to prevent overlap while mapping VM storage onto host files. It introduces the problem of virtualizing the TPM. It creates the possibility that remote attestation may not work. It initiates the problem of detecting VM covert channels. It involves new protection mechanisms for preventing VM escape, VM detection, and VM-VM interference. It initiates the possibility of virtual networking configuration errors. It initiates the risk that malicious software is targeting the VM environment.

It increases overall security risk shared resources, such as networks, clipboards, clocks, printers, desktop management, and folders. Answer A and B are incorrect. These are not the disadvantages of virtualization, as described in the NIST Information Security and Privacy Advisory Board (ISPAB) paper "Perspectives on Cloud Computing and Standards".

NEW QUESTION 24

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

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

Answer: C

Explanation:

An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers, malware and/or disgruntled employees. An IDS cannot directly detect attacks within properly encrypted traffic. An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, trojan horses, and worms). Answer D is incorrect. Access Control List (ACL) is the most commonly used object in Cisco IOS. It filters packets or network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. According to the criteria specified within the access lists, router determines whether the packets to be forwarded or dropped. Access control list criteria could be the source or destination address of the traffic or other information. The types of Cisco ACLs are Standard IP, Extended IP, IPX, Appletalk, etc. Answer B is incorrect. Internet Protocol Security (IPSec) is a method of securing data. It secures traffic by using

encryption and digital signing. It enhances the security of data as if an IPSec packet is captured, its contents cannot be read. IPSec also provides sender verification that ensures the certainty of the datagram's origin to the receiver. Answer A is incorrect. Direct-attached storage (DAS) is a digital storage system that is directly attached to a server or workstation, without using a storage network.

NEW QUESTION 27

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 32

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 34

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

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

Answer: D

Explanation:

The Phase 2 of DITSCAP C&A is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. This phase takes place between the signing of the initial version of the SSAA and the formal accreditation of the system. This phase verifies security requirements during system development. Answer C, B, and A are incorrect. These phases do not take place between the signing of the initial version of the SSAA and the formal accreditation of the system.

NEW QUESTION 39

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

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

Answer: D

Explanation:

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

NEW QUESTION 42

Microsoft software security expert Michael Howard defines some heuristics for determining code review in "A Process for Performing Security Code Reviews".

Which of the following heuristics increase the application's attack surface? Each correct answer represents a complete solution. Choose all that apply.

- A. Code written in C/C++/assembly language
- B. Code listening on a globally accessible network interface
- C. Code that changes frequently
- D. Anonymously accessible code
- E. Code that runs by default
- F. Code that runs in elevated context

Answer: BDEF

Explanation:

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

NEW QUESTION 45

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 48

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 Fraggle Trinoo Tribe Flood Network

NEW QUESTION 50

Which of the following process areas does the SSE-CMM define in the 'Project and Organizational Practices' category? Each correct answer represents a complete solution. Choose all that apply.

- A. Provide Ongoing Skills and Knowledge
- B. Verify and Validate Security
- C. Manage Project Risk
- D. Improve Organization's System Engineering Process

Answer: ACD

Explanation:

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

NEW QUESTION 52

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

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

Answer: C

Explanation:

Password propagation provides an alternative by requiring that a user's authentication credentials be verified by the database before providing access to that user's data. Answer D is incorrect. Account lockout implements a limit on the incorrect password attempts to protect an account from automated password-guessing attacks. Answer B is incorrect. Authenticated session allows a user to access more than one access-restricted Web page without re-authenticating every page. It also integrates user authentication into the basic session model. Answer A is incorrect. Secure assertion distributes application-specific sanity checks throughout the system.

NEW QUESTION 57

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

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

Answer: D

Explanation:

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

NEW QUESTION 61

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

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

Answer: C

Explanation:

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

NEW QUESTION 66

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 68

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

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

Answer: B

Explanation:

The annualized loss expectancy in her project will be \$2,500. Annualized loss expectancy (ALE) is the annually expected financial loss to an organization from a threat. The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as follows: $ALE = \text{Single Loss Expectancy (SLE)} * \text{Annualized Rate of Occurrence (ARO)}$ Here, it is as follows:

$$ALE = SLE * ARO$$

$$= 250,000 * 0.01$$

$$= 2,500$$

Answer D, C, and A are incorrect. These are not valid answers.

NEW QUESTION 69

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

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

Answer: A

Explanation:

A trademark is a name, symbol, or slogan with which a product is identified. Its uniqueness makes the product noticeable among the same type of products. For example, Pentium and Athlon are brand names of the CPUs that are manufactured by Intel and AMD, respectively. The trademark law protects a company's trademark by making it illegal for other companies to use it without taking prior permission of the trademark owner. A trademark is registered so that others cannot use identical or similar marks. Answer C is incorrect. A trade secret is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known. It helps a business to obtain an economic advantage over its competitors or customers. In some jurisdictions, such secrets are referred to as confidential information or classified information. Answer B is incorrect. A copyright is a form of intellectual property, which secures to its holder the exclusive right to produce copies of his or her works of original expression, such as a literary work, movie, musical work or sound recording, painting, photograph, computer program, or industrial design, for a defined, yet extendable, period of time. It does not cover ideas or facts. Copyright laws protect intellectual property from misuse by other individuals. Answer D is incorrect. A patent is a set of exclusive rights granted to anyone who invents any new and useful machine, process, composition of matter, etc. A patent enables the inventor to legally enforce his right to exclude others from using his invention.

NEW QUESTION 73

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 75

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

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

Answer: A

Explanation:

Only acceptance is appropriate for both positive and negative risk events. Often sharing is used for low probability and low impact risk events regardless of the positive or negative effects the risk event may bring the project. Acceptance response is a part of Risk Response planning process. Acceptance response delineates that the project plan will not be changed to deal with the risk. Management may develop a contingency plan if the risk does occur. Acceptance response to a risk event is a strategy that can be used for risks that pose either threats or opportunities. Acceptance response can be of two types: Passive acceptance: It is a strategy in which no plans are made to try or avoid or mitigate the risk. Active acceptance: Such responses include developing contingency reserves to deal with risks, in case they occur. Acceptance is the only response for both threats and opportunities. Answer C is incorrect. Sharing is a positive risk response that shares an opportunity for all parties involved in the risk event. Answer B is incorrect. Transference is a negative risk event that transfers the risk ownership to a third party, such as vendor, through a contractual relationship. Answer D is incorrect. Mitigation is a negative risk event that seeks to lower the probability and/or impact of a risk event.

NEW QUESTION 78

You work as a security engineer for BlueWell Inc. Which of the following documents will you use as a guide for the security certification and accreditation of Federal Information Systems?

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

Answer: C

Explanation:

NIST has developed a suite of documents for conducting Certification & Accreditation (C&A). These documents are as follows: NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems. NIST Special Publication 800-53: This document provides a guideline for security controls for Federal Information Systems. NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System. NIST Special Publication 800-59: This document is a guideline for identifying an information system as a National Security System. NIST Special Publication 800-60: This document is a guide for mapping types of information and information systems to security objectives and risk levels.

NEW QUESTION 83

Which of the following penetration testing techniques automatically tests every phone line in an exchange and tries to locate modems that are attached to the network?

- A. Demon dialing
- B. Sniffing
- C. Social engineering
- D. Dumpster diving

Answer: A

Explanation:

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

NEW QUESTION 88

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 92

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 97

Which of the following types of activities can be audited for security? Each correct answer represents a complete solution. Choose three.

- A. File and object access
- B. Data downloading from the Internet
- C. Printer access
- D. Network logons and logoffs

Answer: ACD

Explanation:

The following types of activities can be audited: Network logons and logoffs File access Printer access Remote access service Application usage Network services Auditing is used to track user accounts for file and object access, logon attempts, system shutdown, etc. This enhances the security of the network. Before enabling security auditing, the type of event to be audited should be specified in the audit policy. Auditing is an essential component to maintain the security of deployed systems. Security auditing depends on the criticality of the environment and on the company's security policy. The security system should be reviewed periodically. Answer B is incorrect. Data downloading from the Internet cannot be audited.

NEW QUESTION 101

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

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

Answer: D

Explanation:

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

NEW QUESTION 104

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 106

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 109

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 110

You work as a security manager for BlueWell Inc. You are going through the NIST SP 800- 37 C&A methodology, which is based on four well defined phases. In which of the following phases of NIST SP 800-37 C&A methodology does the security categorization occur?

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

Answer: D

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 114

You are the project manager of QSL project for your organization. You are working with your project team and several key stakeholders to create a diagram that shows how various elements of a system interrelate and the mechanism of causation within the system. What diagramming technique are you using as a part of the risk identification process?

- A. Cause and effect diagrams
- B. Influence diagrams
- C. Predecessor and successor diagramming
- D. System or process flowcharts

Answer: D

Explanation:

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

NEW QUESTION 118

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

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

Answer: BCD

Explanation:

Following are the various international information security standards: Risk assessment and treatment: Analysis of the organization's information security risks Security policy: Management direction Organization of information security: Governance of information security Asset management: Inventory and classification of information assets Human resources security: Security aspects for employees joining, moving, and leaving an organization Physical and environmental security: Protection of the computer facilities Communications and operations management: Management of technical security controls in systems and networks Access control: Restriction of access rights to networks, systems, applications, functions, and data Information systems acquisition, development and maintenance: Building security into applications Information security incident management: Anticipating and responding appropriately to information security breaches Business continuity management: Protecting, maintaining, and recovering business-critical processes and systems Compliance: Ensuring conformance with information security policies, standards, laws, and regulations Answer A is incorrect. AU audit and accountability is a U.S. Federal Government information security standard.

NEW QUESTION 123

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 127

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 130

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 133

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

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

Answer: B

Explanation:

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

NEW QUESTION 137

Which of the following are the scanning methods used in penetration testing? Each correct answer represents a complete solution. Choose all that apply.

- A. Vulnerability
- B. Port
- C. Services
- D. Network

Answer: ABD

Explanation:

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

Network scanning is a penetration testing activity in which a penetration tester or an attacker identifies active hosts on a network, either to attack them or to perform security assessment. A penetration tester uses various tools to identify all the live or responding hosts on the network and their corresponding IP addresses. Answer B is incorrect. This option comes under vulnerability scanning.

NEW QUESTION 139

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 142

Which of the following vulnerabilities occurs when an application directly uses or concatenates potentially hostile input with data file or stream functions?

- A. Insecure cryptographic storage
- B. Malicious file execution
- C. Insecure communication
- D. Injection flaw

Answer: B

Explanation:

Malicious file execution is a vulnerability that occurs when an application directly uses or concatenates potentially hostile input with data file or stream functions. This leads to arbitrary remote and hostile data being included, processed, and invoked by the Web server. Malicious file execution can be prevented by using an indirect object reference map, input validation, or explicit taint checking mechanism. Answer D is incorrect. Injection flaw occurs when data is sent to an interpreter as a part of command or query. Answer A is incorrect. Insecure cryptographic storage occurs when applications have failed to encrypt data Answer B is incorrect. Insecure communication occurs when applications have failed to encrypt network traffic.

NEW QUESTION 145

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 149

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 154

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 157

Which of the following programming languages are compiled into machine code and directly executed by the CPU of a computer system? Each correct answer represents a complete solution. Choose two.

- A. C
- B. Microsoft.NET
- C. Java EE
- D. C++

Answer: AD

Explanation:

C and C++ programming languages are unmanaged code. Unmanaged code is compiled into machine code and directly executed by the CPU of a computer system. Answer C and B are incorrect. Java EE and Microsoft.Net are compiled into an intermediate code format.

NEW QUESTION 160

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

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

Answer: BCD

Explanation:

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

NEW QUESTION 165

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 169

At which of the following levels of robustness in DRM must the security functions be immune to widely available tools and specialized tools and resistant to professional tools?

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

Answer: C

Explanation:

At Level 1 of robustness in DRM, the security functions must be immune to widely available tools and specialized tools and resistant to professional tools.

NEW QUESTION 173

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 175

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

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

Answer: C

Explanation:

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

NEW QUESTION 178

What are the security advantages of virtualization, as described in the NIST Information Security and Privacy Advisory Board (ISPAB) paper "Perspectives on Cloud Computing and Standards"? Each correct answer represents a complete solution. Choose three.

- A. It increases capabilities for fault tolerant computing.
- B. It adds a layer of security for defense-in-depth.
- C. It decreases exposure of weak software.
- D. It decreases configuration effort.

Answer: ABC

Explanation:

The security advantages of virtualization are as follows: It adds a layer of security for defense-in-depth. It provides strong encapsulation of errors. It increases

intrusion detection through introspection. It decreases exposure of weak software. It increases the flexibility for discovery. It increases capabilities for fault tolerant computing using rollback and snapshot features. Answer D is incorrect. Virtualization increases configuration effort because of complexity of the virtualization layer and composite system.

NEW QUESTION 179

Billy is the project manager of the HAR Project and is in month six of the project. The project is scheduled to last for 18 months. Management asks Billy how often the project team is participating in risk reassessment in this project. What should Billy tell management if he's following the best practices for risk management?

- A. Project risk management happens at every milestone.
- B. Project risk management has been concluded with the project planning.
- C. Project risk management is scheduled for every month in the 18-month project.
- D. At every status meeting the project team project risk management is an agenda item.

Answer: D

Explanation:

Risk management is an ongoing project activity. It should be an agenda item at every project status meeting. Answer A is incorrect. Milestones are good times to do reviews, but risk management should happen frequently. Answer B is incorrect. This answer would only be correct if the project has a status meeting just once per month in the project. Answer B is incorrect. Risk management happens throughout the project as does project planning.

NEW QUESTION 180

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 182

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 186

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 189

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

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

Answer: D

Explanation:

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

NEW QUESTION 193

Which of the following federal agencies has the objective to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life?

- A. National Security Agency (NSA)
- B. National Institute of Standards and Technology (NIST)
- C. United States Congress
- D. Committee on National Security Systems (CNSS)

Answer: B

Explanation:

The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. Answer D is incorrect. The Committee on National Security Systems (CNSS) is a United States intergovernmental organization that sets policy for the security of the US security systems. The CNSS holds discussions of policy issues, sets national policy, directions, operational procedures, and guidance for the information systems operated by the U.S. Government, its contractors, or agents that contain classified information, involve intelligence activities, involve cryptographic activities related to national security, etc. Answer A is incorrect. The National Security Agency/Central Security Service (NSA/CSS) is a crypto-logic intelligence agency of the United States government. It is administered as part of the United States Department of Defense. NSA is responsible for the collection and analysis of foreign communications and foreign signals intelligence, which involves cryptanalysis. NSA is also responsible for protecting U.S. government communications and information systems from similar agencies elsewhere, which involves cryptography. NSA is a key component of the U.S. Intelligence Community, which is headed by the Director of National Intelligence. The Central Security Service is a co-located agency created to coordinate intelligence activities and co-operation between NSA and U.S. military cryptanalysis agencies. NSA's work is limited to communications intelligence. It does not perform field or human intelligence activities. Answer B is incorrect. The United States Congress is the bicameral legislature of the federal government of the United States of America. It consists of the Senate and the House of Representatives. The Congress meets in the United States Capitol in Washington, D.C. Both senators and representatives are chosen through direct election. Each of the 435 members of the House of Representatives represents a district and serves a two-year term. House seats are apportioned among the states by population. The 100 Senators serve staggered six-year terms. Each state has two senators, regardless of population. Every two years, approximately one-third of the Senate is elected at a time. The United States Congress main function is to make laws. The Office of the Law Revision Counsel organizes and publishes the United States Code (USC). It is a consolidation and codification by subject matter of the general and permanent laws of the United States.

NEW QUESTION 194

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 196

NIST SP 800-53A defines three types of interview depending on the level of assessment conducted. Which of the following NIST SP 800-53A interviews consists of informal and ad hoc interviews?

- A. Comprehensive
- B. Significant
- C. Abbreviated
- D. Substantial

Answer: C

Explanation:

Abbreviated interview consists of informal and ad hoc interviews. Answer D is incorrect. Substantial interview consists of informal and structured interviews. Answer A is incorrect. Comprehensive interview consists of formal and structured interviews. Answer B is incorrect. There is no such type of interview in NIST SP 800-53A.

NEW QUESTION 198

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

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

Answer: D

Explanation:

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

NEW QUESTION 199

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 200

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 203

John works as a security manager for SoftTech Inc. He is working with his team on the disaster recovery management plan. One of his team members has a doubt related to the most cost effective DRP testing plan. According to you, which of the following disaster recovery testing plans is the most cost-effective and efficient way to identify areas of overlap in the plan before conducting more demanding training exercises?

- A. Full-scale exercise
- B. Walk-through drill
- C. Structured walk-through test
- D. Evacuation drill

Answer: C

Explanation:

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

NEW QUESTION 204

Which of the following US Acts emphasized a "risk-based policy for cost-effective security" and makes mandatory for agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget?

- A. Federal Information Security Management Act of 2002 (FISMA)
- B. The Electronic Communications Privacy Act of 1986 (ECPA)
- C. The Equal Credit Opportunity Act (ECOA)

D. The Fair Credit Reporting Act (FCRA)

Answer: A

Explanation:

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

NEW QUESTION 206

"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 210

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

- A. The quantitative risk analysis process will analyze the effect of risk events that may substantially impact the project's competing demands.
- B. The quantitative risk analysis reviews the results of risk identification and prepares the project for risk response management.
- C. The quantitative risk analysis seeks to determine the true cost of each identified risk event and the probability of each risk event to determine the risk exposure.
- D. The quantitative risk analysis process will review risk events for their probability and impact on the project objectives.

Answer: A

Explanation:

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

NEW QUESTION 212

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

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

Answer: A

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 213

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

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

Answer: C

Explanation:

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

NEW QUESTION 217

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

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

Answer: ABCD

Explanation:

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

NEW QUESTION 218

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 222

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 224

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 226

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

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

Answer: C

Explanation:

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

NEW QUESTION 228

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

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

Answer: CD

Explanation:

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

NEW QUESTION 229

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

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

Answer: B

Explanation:

NIST has developed a suite of documents for conducting Certification & Accreditation (C&A). These documents are as follows: NIST Special Publication 800-37:

This document is a guide for the security certification and accreditation of Federal Information Systems. NIST Special Publication 800-53: This document provides a guideline for security controls for Federal Information Systems. NIST Special Publication 800-53A: This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System. NIST Special Publication 800-59: This document is a guideline for identifying an information system as a National Security System. NIST Special Publication 800-60: This document is a guide for mapping types of information and information systems to security objectives and risk levels.

NEW QUESTION 230

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 233

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

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

Answer: ACD

Explanation:

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

NEW QUESTION 234

Which of the following terms refers to a mechanism which proves that the sender really sent a particular message?

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

Answer: B

Explanation:

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

NEW QUESTION 238

Which of the following allows multiple operating systems (guests) to run concurrently on a host computer?

- A. Emulator
- B. Hypervisor
- C. Grid computing
- D. CP/CMS

Answer: B

Explanation:

A hypervisor is a virtualization technique that allows multiple operating systems (guests) to run concurrently on a host computer. It is also called the virtual machine monitor (VMM). The hypervisor provides a virtual operating platform to the guest operating systems and checks their execution process. It provides isolation to the host's resources. The hypervisor is installed on server hardware. Answer A is incorrect. Emulator duplicates the functions of one system using a different system, so that the second system behaves like the first system. Answer D is incorrect. CP/CMS is a time-sharing operating system of the late 60s and early 70s, and it is known for its excellent performance and advanced features. Answer B is incorrect. Grid computing refers to the combination of computer resources from multiple administrative domains to achieve a common goal.

NEW QUESTION 242

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

- A. Least privilege
- B. Economy of mechanism
- C. Psychological acceptability
- D. Separation of duties

Answer: B

Explanation:

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

NEW QUESTION 244

Which of the following disaster recovery tests includes the operations that shut down at the primary site, and are shifted to the recovery site according to the disaster recovery plan?

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

Answer: B

Explanation:

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

NEW QUESTION 246

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

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

Answer: C

Explanation:

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

NEW QUESTION 247

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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 First Try
- * CSSLP Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CSSLP Practice Test Here](#)