

ISC2

Exam Questions CSSLP

Certified Information Systems Security Professional



NEW QUESTION 1

The organization level is the Tier 1 and it addresses risks from an organizational perspective. What are the various Tier 1 activities? Each correct answer represents a complete solution. Choose all that apply.

- A. The organization plans to use the degree and type of oversight, to ensure that the risk management strategy is being effectively carried out.
- B. The level of risk tolerance.
- C. The techniques and methodologies an organization plans to employ, to evaluate information system-related security risks.
- D. The RMF primarily operates at Tier 1.

Answer: ABC

Explanation:

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

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

NEW QUESTION 2

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 3

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 4

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

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

Answer: C

Explanation:

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

NEW QUESTION 5

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

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

Answer: A

Explanation:

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

NEW QUESTION 6

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 7

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

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

Answer: AC

Explanation:

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

NEW QUESTION 8

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

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

Answer: A

Explanation:

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

NEW QUESTION 9

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

- A. Espionage law
- B. Trademark law
- C. Cyber law

D. Copyright law

Answer: B

Explanation:

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

NEW QUESTION 10

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

- A. Cold Site
- B. Hot Site
- C. Warm Site
- D. Mobile Site

Answer: B

Explanation:

A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data. It provides the backup facility, which is maintained in a constant order, with a full complement of servers, workstations, and communication links ready to assume the primary operations responsibility.

A hot site is a backup site in case disaster has taken place in a data center. A hot site is located off site and provides the best protection. It is an exact replica of the current data center. In case a disaster struck to the data center, administrators just need to take the backup of recent data in hot site and the data center is back online in a very short time. It is very expensive to create and maintain the hot site. There are lots of third party companies that provide disaster recovery solutions by maintaining hot sites at their end. Answer A is incorrect. A cold site is a backup site in case disaster has taken place in a data center. This is the least expensive disaster recovery solution, usually having only a single room with no equipment. All equipment is brought to the site after the disaster. It can be on site or off site. Answer D is incorrect. Mobile sites are self-reliant, portable shells custom-fitted with definite telecommunications and IT equipment essential to meet system requirements. These are presented for lease through commercial vendors. Answer C is incorrect. A warm site is, quite logically, a compromise between hot and cold sites. Warm sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. These sites will have backups on hand, but they may not be complete and may be between several days and a week old. An example would be backup tapes sent to the warm site by courier.

NEW QUESTION 10

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 13

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

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

D. Qualitative risk analysis

Answer: A

Explanation:

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

NEW QUESTION 17

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

- A. What is being secured?
- B. Where is the vulnerability, threat, or risk?
- C. Who is expected to exploit the vulnerability?
- D. Who is expected to comply with the policy?

Answer: ABD

Explanation:

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

NEW QUESTION 20

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

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

Answer: C

Explanation:

Detection risks are the risks that an auditor will not be able to find what they are looking to detect. Hence, it becomes tedious to report negative results when material conditions (faults) actually exist. Detection risk includes two types of risk: Sampling risk: This risk occurs when an auditor falsely accepts or erroneously rejects an audit sample. Nonsampling risk: This risk occurs when an auditor fails to detect a condition because of not applying the appropriate procedure or using procedures inconsistent with the audit objectives (detection faults). Answer A is incorrect. Residual risk is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures). The formula to calculate residual risk is (inherent risk) x (control risk) where inherent risk is (threats vulnerability). In the economic context, residual means "the quantity left over at the end of a process; a remainder". Answer D is incorrect. Inherent risk, in auditing, is the risk that the account or section being audited is materially misstated without considering internal controls due to error or fraud. The assessment of inherent risk depends on the professional judgment of the auditor, and it is done after assessing the business environment of the entity being audited. Answer B is incorrect. A secondary risk is a risk that arises as a straight consequence of implementing a risk response. The secondary risk is an outcome of dealing with the original risk. Secondary risks are not as rigorous or important as primary risks, but can turn out to be so if not estimated and planned properly.

NEW QUESTION 25

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 27

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

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

Answer: C

Explanation:

2Mosaic is a tool used for watermark breaking. It is an attack against a digital watermarking system. In this type of attack, an image is chopped into small pieces

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

NEW QUESTION 28

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 31

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

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

Answer: C

Explanation:

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

NEW QUESTION 35

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 40

Which of the following is a malicious exploit of a website, whereby unauthorized commands are transmitted from a user trusted by the website?

- A. Cross-Site Scripting

- B. Injection flaw
- C. Side channel attack
- D. Cross-Site Request Forgery

Answer: D

Explanation:

CSRF (Cross-Site Request Forgery) is a malicious exploit of a website, whereby unauthorized commands are transmitted from a user trusted by the website. It is also known as a one-click attack or session riding. CSRF occurs when a user is tricked by an attacker into activating a request in order to perform some unauthorized action. It increases data loss and malicious code execution. Answer A is incorrect. Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which enable malicious attackers to inject client-side script into web pages viewed by other users. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls, such as the same origin policy. Cross-site scripting carried out on websites were roughly 80% of all security vulnerabilities documented by Symantec as of 2007. Their impact may range from a petty nuisance to a significant security risk, depending on the sensitivity of the data handled by the vulnerable site, and the nature of any security mitigations implemented by the site owner. Answer C is incorrect. A side channel attack is based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms (compare cryptanalysis). For example, timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information which can be exploited to break the system. Many side-channel attacks require considerable technical knowledge of the internal operation of the system on which the cryptography is implemented. Answer B is incorrect. Injection flaws are the vulnerabilities where a foreign agent illegally uses a sub-system. They are the vulnerability holes that can be used to attack a database of Web applications. It is the most common technique of attacking a database. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing involuntary commands or changing data. Injection flaws include XSS (HTML Injection) and SQL Injection.

NEW QUESTION 41

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

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

Answer: C

Explanation:

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

NEW QUESTION 42

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

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

Answer: B

Explanation:

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

NEW QUESTION 44

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 48

The Software Configuration Management (SCM) process defines the need to trace changes, and the ability to verify that the final delivered software has all of the planned enhancements that are supposed to be included in the release. What are the procedures that must be defined for each software project to ensure that a sound SCM process is implemented? Each correct answer represents a complete solution. Choose all that apply.

- A. Configuration status accounting
- B. Configuration change control
- C. Configuration identification
- D. Configuration audits
- E. Configuration implementation
- F. Configuration deployment

Answer: ABCD

Explanation:

The SCM process defines the need to trace changes, and the ability to verify that the final delivered software has all of the planned enhancements that are supposed to be included in the release. It identifies four procedures that must be defined for each software project to ensure that a sound SCM process is implemented. They are as follows:

- * 1. Configuration identification: 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.
- * 2. Configuration change control: Configuration change control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them.
- * 3. Configuration status accounting: Configuration status accounting is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time.
- * 4. Configuration audits: Configuration audits are broken into functional and physical configuration audits. They occur either at delivery or at the moment of effecting the change. A functional configuration audit ensures that functional and performance attributes of a configuration item are achieved, while a physical configuration audit ensures that a configuration item is installed in accordance with the requirements of its detailed design documentation.

NEW QUESTION 53

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

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

Answer: D

Explanation:

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

NEW QUESTION 57

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 59

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 61

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

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

Answer: AD

Explanation:

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

NEW QUESTION 64

In which of the following architecture styles does a device receive input from connectors and generate transformed outputs?

- A. N-tiered
- B. Heterogeneous
- C. Pipes and filters
- D. Layered

Answer: C

Explanation:

In the pipes and filters architecture style, a device receives input from connectors and generates transformed outputs. A pipeline has a series of processing elements in which the output of each element works as an input of the next element. A little amount of buffering is provided between the two successive elements.

NEW QUESTION 67

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

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

Answer: ABDF

Explanation:

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

NEW QUESTION 70

Which of the following programming languages are compiled into machine code and directly executed by the CPU of a computer system? Each correct answer

represents a complete solution. Choose two.

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

Answer: 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 71

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

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

Answer: A

Explanation:

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

NEW QUESTION 76

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 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 81

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

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

Answer: D

Explanation:

The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk. The Certification Determination and Accreditation phase is the third phase in the DIACAP process. Its subordinate tasks are as follows: Analyze residual risk. Issue certification determination. Make accreditation decision. Answer A is incorrect. Phase 1 is known as Initiate and Plan IA C&Answer B is incorrect. Phase 2 is used to implement and validate assigned IA controls. Answer E is incorrect. Phase 3 is used to make certification determination and accreditation decisions. Answer B is incorrect. Phase 5 is known as decommission system and is used to conduct activities related to the disposition of the system data and objects.

NEW QUESTION 83

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

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

Answer: BD

Explanation:

FISMA and Office of Management and Budget (OMB) require all general support systems and major applications to be fully certified and accredited before they are put into production. General support systems and major applications are also referred to as information systems and are required to be reaccredited every three years. Answer A is incorrect. The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. Answer B is incorrect. The Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States federal government for use by all non-military government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community (ANSI, IEEE, ISO, etc.). Some FIPS standards were originally developed by the U.S. government. For instance, standards for encoding data (e.g., country codes), but more significantly some encryption standards, such as the Data Encryption Standard (FIPS 46-3) and the Advanced Encryption Standard (FIPS 197). In 1994, NOAA (Noaa) began broadcasting coded signals called FIPS (Federal Information Processing System) codes along with their standard weather broadcasts from local stations. These codes identify the type of emergency and the specific geographic area (such as a county) affected by the emergency.

NEW QUESTION 87

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

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

Answer: D

Explanation:

BCP is a strategy to minimize the consequence of the instability and to allow for the continuation of business processes. The goal of BCP is to minimize the effects of a disruptive event on a company, and is formed to avoid interruptions to normal business activity. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan. Answer B is incorrect. A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and "triggers" for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption. Answer B is incorrect. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication, and reputation protection, and should refer to the disaster recovery plan (DRP) for IT-related infrastructure recovery/continuity. Answer A is incorrect. The Continuity Of Operation Plan (COOP) refers to the preparations and institutions maintained by the United States government, providing survival of federal government operations in the case of catastrophic events. It provides procedures and capabilities to sustain an organization's essential. COOP is the procedure documented to ensure persistent critical operations throughout any period where normal operations are unattainable.

NEW QUESTION 92

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

- A. It specifies the various levels of robustness that are needed for asset security.
- B. It specifies minimum techniques for asset security.
- C. It specifies the behaviors of the DRM implementation and applications accessing the implementation.
- D. It contains assets, such as device key, content key, algorithm, and profiling data.

Answer: ABD

Explanation:

The DRM (digital rights management) technology includes the following rules: 1.Compliance rule: This rule specifies the behaviors of the DRM implementation, and applications that are accessing the implementation. The compliance rule specifies the following elements: Definition of specific license rights Device requirements Revocation of license path or penalties when the implementation is not robust enough or noncompliant 2.Robustness rule: This rule has the following features: It specifies the various levels of robustness that are needed for asset security. It contains assets, such as device key, content key, algorithm, and profiling data. It specifies minimum techniques for asset security.

NEW QUESTION 96

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 97

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 99

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 100

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 105

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

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

Answer: ACD

Explanation:

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

NEW QUESTION 110

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

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

Answer: ACD

Explanation:

The following are the responsibilities of the owner with regard to data in an information classification program: Determining what level of classification the information requires. Reviewing the classification assignments at regular time intervals and making changes as the business needs change. Delegating the

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

NEW QUESTION 114

Fill in the blank with an appropriate phrase. A is defined as any activity that has an effect on defining, designing, building, or executing a task, requirement, or procedure.

A. technical effort

Answer: A

Explanation:

A technical effort is described as any activity, which has an effect on defining, designing, building, or implementing a task, requirement, or procedure. The technical effort is an element of technical management that is required to progress efficiently and effectively from a business need to the deployment and operation of the system.

NEW QUESTION 118

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

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

Answer: C

Explanation:

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

NEW QUESTION 121

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 126

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 131

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

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

Answer: D

Explanation:

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

NEW QUESTION 132

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 135

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 140

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 143

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 147

The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise. What are the responsibilities of a Chief Information Officer? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BCD

Explanation:

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

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

NEW QUESTION 151

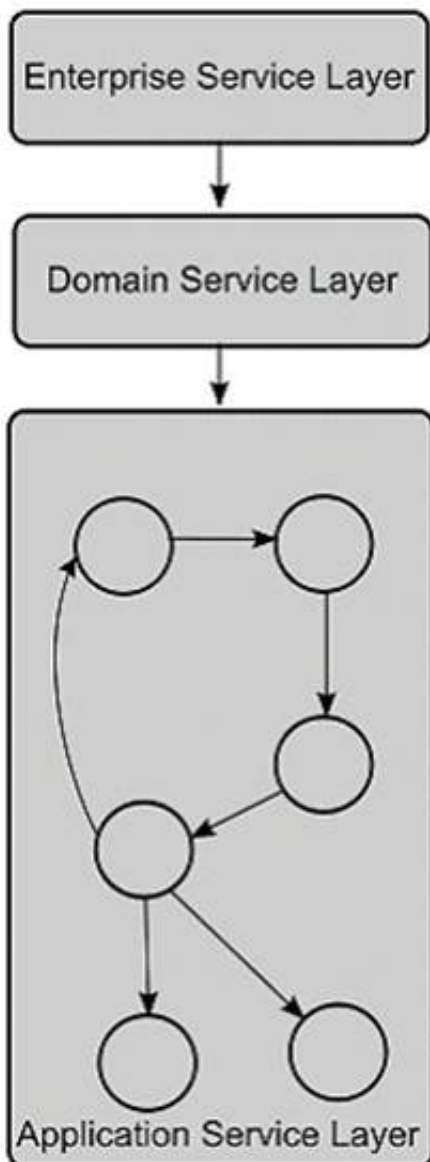
Which of the following security architectures defines how to integrate widely disparate applications for a world that is Web-based and uses multiple implementation platforms?

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

Answer: C

Explanation:

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



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

NEW QUESTION 155

Which of the following is an attack with IP fragments that cannot be reassembled?

- A. Password guessing attack
- B. Teardrop attack
- C. Dictionary attack
- D. Smurf attack

Answer: B

Explanation:

Teardrop is an attack with IP fragments that cannot be reassembled. In this attack, corrupt packets are sent to the victim's computer by using IP's packet fragmentation algorithm. As a result of this attack, the victim's computer might hang. Answer D is incorrect. Smurf is an ICMP attack that involves spoofing and flooding. Answer B is incorrect. Dictionary attack is a type of password guessing attack. This type of attack uses a dictionary of common words to find out the password of a user. It can also use common words in either upper or lower case to find a password. There are many programs available on the Internet to automate and execute dictionary attacks. Answer A is incorrect. A password guessing attack occurs when an unauthorized user tries to log on repeatedly to a computer or network by guessing usernames and passwords. Many password guessing programs that attempt to break passwords are available on the Internet. Following are the types of password guessing attacks: Brute force attack Dictionary attack

NEW QUESTION 156

Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in. What are the different categories of penetration testing? Each correct answer represents a complete solution. Choose all that apply.

- A. Open-box
- B. Closed-box
- C. Zero-knowledge test
- D. Full-box
- E. Full-knowledge test
- F. Partial-knowledge test

Answer: ABCEF

Explanation:

The different categories of penetration testing are as follows: Open-box: In this category of penetration testing, testers have access to internal system code. This mode is basically suited for Unix or Linux. Closed-box: In this category of penetration testing, testers do not have access to closed systems. This method is good for closed systems. Zero-knowledge test: In this category of penetration testing, testers have to acquire information from scratch and they are not supplied with information concerning the IT system. Partial-knowledge test: In this category of penetration testing, testers have knowledge that may be applicable to a specific type of attack and associated vulnerabilities. Full-knowledge test: In this category of penetration testing, testers have massive knowledge concerning the

information system to be evaluated. Answer D is incorrect. There is no such category of penetration testing.

NEW QUESTION 159

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

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

Answer: D

Explanation:

The Federal Information Security Management Act of 2002 is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002. The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA has brought attention within the federal government to cybersecurity and explicitly emphasized a 'risk-based policy for cost-effective security'. FISMA requires agency program officials, chief information officers, and Inspectors Generals (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget (OMB). OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act. Answer B is incorrect. The Lanham Act is a piece of legislation that contains the federal statutes of trademark law in the United States. The Act prohibits a number of activities, including trademark infringement, trademark dilution, and false advertising. It is also called Lanham Trademark Act. Answer A is incorrect. The Computer Misuse Act 1990 is an act of the UK Parliament which states the following statement: Unauthorized access to the computer material is punishable by 6 months imprisonment or a fine "not exceeding level 5 on the standard scale" (currently 5000). Unauthorized access with the intent to commit or facilitate commission of further offences is punishable by 6 months/maximum fine on summary conviction or 5 years/fine on indictment. Unauthorized modification of computer material is subject to the same sentences as section 2 offences. Answer B is incorrect. The Computer Fraud and Abuse Act is a law passed by the United States Congress in 1984 intended to reduce cracking of computer systems and to address federal computer-related offenses. The Computer Fraud and Abuse Act (codified as 18 U.S.C. 1030) governs cases with a compelling federal interest, where computers of the federal government or certain financial institutions are involved, where the crime itself is interstate in nature, or computers used in interstate and foreign commerce. It was amended in 1986, 1994, 1996, in 2001 by the USA PATRIOT Act, and in 2008 by the Identity Theft Enforcement and Restitution Act. Section (b) of the act punishes anyone who not just commits or attempts to commit an offense under the Computer Fraud and Abuse Act but also those who conspire to do so.

NEW QUESTION 164

Security Test and Evaluation (ST&E) is a component of risk assessment. It is useful in discovering system vulnerabilities. For what purposes is ST&E used? Each correct answer represents a complete solution. Choose all that apply.

- A. To implement the design of system architecture
- B. To determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy
- C. To assess the degree of consistency between the system documentation and its implementation
- D. To uncover design, implementation, and operational flaws that may allow the violation of security policy

Answer: BCD

Explanation:

Security Test and Evaluation (ST&E) is a component of risk assessment. It is useful in discovering system vulnerabilities. According to NIST SP 800-42 (Guideline on Network Security Testing), ST&E is used for the following purposes: To assess the degree of consistency between the system documentation and its implementation To determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy To uncover design, implementation, and operational flaws that may allow the violation of security policy Answer A is incorrect. ST&E is not used for the implementation of the system architecture.

NEW QUESTION 168

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

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

Answer: D

Explanation:

Phase 4, Post Accreditation Phase, of the DITSCAP includes the activities that are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle. Answer 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 A is incorrect. Phase 2, Verification, verifies the evolving or modified system's compliance with the information agreed on in the System Security Authorization Agreement (SSAA). Answer B is incorrect. Phase 3 validates the compliance of a fully integrated system with the information stated in the SSAA.

NEW QUESTION 170

Which of the following documents is defined as a source document, which is most useful for the ISSE when classifying the needed security functionality?

- A. Information Protection Policy (IPP)
- B. IMM
- C. System Security Context
- D. CONOPS

Answer: A

Explanation:

The Information Protection Policy (IPP) is defined as a source document, which is most useful for the ISSE when classifying the needed security functionality. The IPP document consists of the threats to the information management and the security services and controls needed to respond to those threats. Answer B is incorrect. The IMM is the source document describing the customer's needs based on identifying users, processes, and information. Answer B is incorrect. The System Security Context is the output of SE and ISSEP. It is the translation of the requirements into system parameters and possible measurement concepts that meet the defined requirements. Answer D is incorrect. The Concept of Operations (CONOPS) is a document describing the characteristics of a proposed system from the viewpoint of an individual who will use that system. It is used to communicate the quantitative and qualitative system characteristics to all stakeholders. CONOPS are widely used in the military or in government services, as well as other fields. A CONOPS generally evolves from a concept and is a description of how a set of capabilities may be employed to achieve desired objectives or a particular end state for a specific scenario.

NEW QUESTION 175

Who amongst the following makes the final accreditation decision?

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

Answer: C

Explanation:

The DAA, also known as Authorizing Official, makes the final accreditation decision. The Designated Approving Authority (DAA), in the United States Department of Defense, is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. The DAA is responsible for implementing system security. The DAA can grant the accreditation and can determine that the system's risks are not at an acceptable level and the system is not ready to be operational. Answer D is incorrect. An Information System Security Officer (ISSO) plays the role of a supporter. The responsibilities of an Information System Security Officer (ISSO) are as follows: Manages the security of the information system that is slated for Certification & Accreditation (C&A). Insures the information systems configuration with the agency's information security policy. Supports the information system owner/information owner for the completion of security-related responsibilities. Takes part in the formal configuration management process. Prepares Certification & Accreditation (C&A) packages. Answer A is incorrect. An Information System Security Engineer (ISSE) plays the role of an advisor. The responsibilities of an Information System Security Engineer are as follows: Provides view on the continuous monitoring of the information system. Provides advice on the impacts of system changes. Takes part in the configuration management process. Takes part in the development activities that are required to implement system changes. Follows approved system changes. Answer B is incorrect. A Chief Risk Officer (CRO) is also known as Chief Risk Management Officer (CRMO). The Chief Risk Officer or Chief Risk Management Officer of a corporation is the executive accountable for enabling the efficient and effective governance of significant risks, and related opportunities, to a business and its various segments. Risks are commonly categorized as strategic, reputational, operational, financial, or compliance-related. CRO's are accountable to the Executive Committee and The Board for enabling the business to balance risk and reward. In more complex organizations, they are generally responsible for coordinating the organization's Enterprise Risk Management (ERM) approach.

NEW QUESTION 179

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

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

Answer: D

Explanation:

The Bell-La Padula Model is a state machine model used for enforcing access control in government and military applications. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g., "Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public"). The Bell-La Padula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity. Answer B is incorrect. The Biba model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject. Answer A is incorrect. The Clark-Wilson model provides a foundation for specifying and analyzing an integrity policy for a computing system. The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. The model's enforcement and certification rules define data items and processes that provide the basis for an integrity policy. The core of the model is based on the notion of a transaction. Answer B is incorrect. The take-grant protection model is a formal model used in the field of computer security to establish or disprove the safety of a given computer system that follows specific rules. It shows that for specific systems the question of safety is decidable in linear time, which is in general undecidable. The model represents a system as directed graph, where vertices are either subjects or objects. The edges between them are labeled and the label indicates the rights that the source of the edge has over the destination. Two rights occur in every instance of the model: take and grant. They play a special role in the graph rewriting rules describing admissible changes of the graph.

NEW QUESTION 181

Which of the following refers to the ability to ensure that the data is not modified or tampered with?

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

Answer: A

Explanation:

Integrity refers to the ability to ensure that the data is not modified or tampered with. Integrity means that data cannot be modified without authorization. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a Web site, when someone is able to cast a very large number of votes in an online poll, and so on. Answer D is incorrect. Confidentiality is the property of preventing disclosure of information to unauthorized individuals or systems. Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on

it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Answer B is incorrect. Availability means that data must be available whenever it is needed. Answer B is incorrect. Non-repudiation is the concept of ensuring that a party in a dispute cannot refuse to acknowledge, or refute the validity of a statement or contract. As a service, it provides proof of the integrity and origin of data. Although this concept can be applied to any transmission, including television and radio, by far the most common application is in the verification and trust of signatures.

NEW QUESTION 183

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

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

Answer: D

Explanation:

According to the question, you are hiring a local expert team for casting the column. As you have transferred your risk to a third party, this is the transference risk response that you have adopted. Transference is a strategy to mitigate negative risks or threats. In this strategy, consequences and the ownership of a risk is transferred to a third party. This strategy does not eliminate the risk but transfers responsibility of managing the risk to another party. Insurance is an example of transference. Answer B is incorrect. Mitigation is a risk response planning technique associated with threats that seeks to reduce the probability of occurrence or impact of a risk to below an acceptable threshold. Risk mitigation involves taking early action to reduce the probability and impact of a risk occurring on the project. Adopting less complex processes, conducting more tests, or choosing a more stable supplier are examples of mitigation actions. Answer A is incorrect. Avoidance involves changing the project management plan to eliminate the threat entirely. Answer B is incorrect. Acceptance response is a part of Risk Response planning process. Acceptance response delineates that the project plan will not be changed to deal with the risk. Management may develop a contingency plan if the risk does occur. Acceptance response to a risk event is a strategy that can be used for risks that pose either threats or opportunities. Acceptance response can be of two types: Passive acceptance: It is a strategy in which no plans are made to try or avoid or mitigate the risk. Active acceptance: Such responses include developing contingency reserves to deal with risks, in case they occur. Acceptance is the only response for both threats and opportunities.

NEW QUESTION 186

Which of the following describes the acceptable amount of data loss measured in time?

- A. Recovery Point Objective (RPO)
- B. Recovery Time Objective (RTO)
- C. Recovery Consistency Objective (RCO)
- D. Recovery Time Actual (RTA)

Answer: A

Explanation:

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

NEW QUESTION 188

A part of a project deals with the hardware work. As a project manager, you have decided to hire a company to deal with all hardware work on the project. Which type of risk response is this?

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

Answer: C

Explanation:

When you are hiring a third party to own risk, it is known as transference risk response. Transference is a strategy to mitigate negative risks or threats. In this strategy, consequences and the ownership of a risk is transferred to a third party. This strategy does not eliminate the risk but transfers responsibility of managing the risk to another party. Insurance is an example of transference. Answer B is incorrect. The act of spending money to reduce a risk probability and impact is known as mitigation. Answer A is incorrect. Exploit is a strategy that may be selected for risks with positive impacts where the organization wishes to ensure that the opportunity is realized. Answer D is incorrect. When extra activities are introduced into the project to avoid the risk, this is an example of avoidance.

NEW QUESTION 192

You work as a CSO (Chief Security Officer) for Tech Perfect Inc. You want to perform the following tasks: Develop a risk-driven enterprise information security architecture. Deliver security infrastructure solutions that support critical business initiatives. Which of the following methods will you use to accomplish these tasks?

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

Answer: C

Explanation:

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

NEW QUESTION 193

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

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

Answer: C

Explanation:

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

NEW QUESTION 197

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

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

Answer: A

Explanation:

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

If the asset is completely lost, the Exposure Factor is 1.0. The result is a monetary value in the same unit as the Single Loss Expectancy is expressed. Here, it is as follows:

$$\begin{aligned} \text{SLE} &= \text{Asset Value} * \text{Exposure Factor} \\ &= 195,000 * 0.35 \\ &= \$68,250 \end{aligned}$$

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

NEW QUESTION 199

DRAG DROP

RCA (root cause analysis) is an iterative and reactive method that identifies the root cause of various incidents, and the actions required to prevent these incidents from reoccurring. RCA is classified in various categories. Choose appropriate categories and drop them in front of their respective functions.

RCA categories	Functions	
Drop Here	It consists of plans from the health and safety areas.	Safety-based RCA
Drop Here	It integrates quality control paradigms.	Production-based RCA
Drop Here	It integrates business processes.	Process-based RCA
Drop Here	It integrates failure analysis processes.	Failure-based RCA
Drop Here	It integrates the methods from risk and systems analysis.	Systems-based RCA

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

The various categories of root cause analysis (RCA) are as follows: Safety-based RC A. It consists of plans from the health and safety areas. Production-based RCA. It integrates quality control paradigms. Process-based RCA. It integrates business processes. Failure- based RCA. It integrates failure analysis processes as employed in engineering and maintenance. Systems-based RCA. It integrates the methods from risk and systems analysis.

NEW QUESTION 200

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

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

Answer: B

Explanation:

Audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function. Audit records typically result from activities such as transactions or communications by individual people, systems, accounts, or other entities. The process that creates audit trail should always run in a privileged mode, so it could access and supervise all actions from all users, and normal user could not stop/change it. Furthermore, for the same reason, trail file or database table with a trail should not be accessible to normal users. Answer B is incorrect. A computer security audit is a manual or systematic measurable technical assessment of a system or application. Manual assessments include interviewing staff, performing security vulnerability scans, reviewing application and operating system access controls, and analyzing physical access to the systems. Automated assessments, or CAAT's, include system generated audit reports or using software to monitor and report changes to files and settings on a system. Systems can include personal computers, servers, mainframes, network routers, and switches. Answer D is incorrect. Detective controls are the audit controls that are not needed to be restricted. Any control that performs a monitoring activity can likely be defined as a Detective Control. For example, it is possible that mistakes, either intentional or unintentional, can be made. Therefore, an additional Protective control is that these companies must have their financial results audited by an independent Certified Public Accountant. The role of this accountant is to act as an auditor. In fact, any auditor acts as a Detective control. If the organization in question has not properly followed the rules, a diligent auditor should be able to detect the deficiency which indicates that some control somewhere has failed. Answer A is incorrect. Reactive or corrective controls typically work in response to a detective control, responding in such a way as to alert or otherwise correct an unacceptable condition. Using the example of account rules, either the internal Audit Committee or the SEC itself, based on the report generated by the external auditor, will take some corrective action. In this way, they are acting as a Corrective or Reactive control.

NEW QUESTION 204

Fill in the blank with an appropriate phrase The is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity.

- A. Biba model

Answer: A

Explanation:

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 209

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

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

Answer: C

Explanation:

The risk management plan defines the roles and responsibilities for conducting risk management. A Risk management plan is a document arranged by a project

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

NEW QUESTION 210

In 2003, NIST developed a new Certification & Accreditation (C&A) guideline known as FIPS 199. What levels of potential impact are defined by FIPS 199? Each correct answer represents a complete solution. Choose all that apply.

- A. Moderate
- B. Medium
- C. High
- D. Low

Answer: BCD

Explanation:

In 2003, NIST developed a new Certification & Accreditation (C&A) guideline known as FIPS 199. FIPS 199 is a standard for security categorization of Federal Information and Information Systems. It defines three levels of potential impact: Low: It causes a limited adverse effect. Medium: It causes a serious adverse effect. High: It causes a severe adverse effect.

NEW QUESTION 212

You work as a security manager for BlueWell Inc. You are performing the external vulnerability testing, or penetration testing to get a better snapshot of your organization's security posture. Which of the following penetration testing techniques will you use for searching paper disposal areas for unshredded or otherwise improperly disposed-of reports?

- A. Sniffing
- B. Scanning and probing
- C. Dumpster diving
- D. Demon dialing

Answer: C

Explanation:

Dumpster diving technique is used for searching paper disposal areas for unshredded or otherwise improperly disposed-of reports. Answer B is incorrect. In scanning and probing technique, various scanners, like a port scanner, can reveal information about a network's infrastructure and enable an intruder to access the network's unsecured ports. Answer D is incorrect. Demon dialing technique automatically tests every phone line in an exchange to try to locate modems that are attached to the network. Answer A is incorrect. In sniffing technique, protocol analyzer can be used to capture data packets that are later decoded to collect information such as passwords or infrastructure configurations.

NEW QUESTION 216

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

- A. It ensures that unauthorized modifications are not made to data by authorized personnel or processes.
- B. It determines the actions and behaviors of a single individual within a system
- C. It ensures that internal information is consistent among all subentities and also consistent with the real-world, external situation.
- D. It ensures that modifications are not made to data by unauthorized personnel or processes.

Answer: ACD

Explanation:

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

NEW QUESTION 220

.....

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](#)