Exam Questions CSSLP

Certified Information Systems Security Professional

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

NEW QUESTION 1
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 2
You are the project manager of the CUL project in your organization. You and the project team are assessing the risk events and creating a probability and impact matrix for the identified risks. Which one of the following statements best describes the requirements for the data type used in qualitative risk analysis?

A. A qualitative risk analysis encourages biased data to reveal risk tolerances.
B. A qualitative risk analysis required unbiased stakeholders with biased risk tolerances.
C. A qualitative risk analysis requires accurate and unbiased data if it is to be credible.
D. A qualitative risk analysis requires fast and simple data to complete the analysis.

Answer: C

Explanation:
Of all the choices only this answer is accurate. The PMBOK clearly states that the data must be accurate and unbiased to be credible. Answer D is incorrect. This is not a valid statement about the qualitative risk analysis datAnswer A is incorrect. This is not a valid statement about the qualitative risk analysis datAnswer B is incorrect. This is not a valid statement about the qualitative risk analysis data.

NEW QUESTION 3
Which of the following coding practices are helpful in simplifying code? Each correct answer represents a complete solution. Choose all that apply.

A. Programmers should use multiple small and simple functions rather than a single complex function.
B. Software should avoid ambiguities and hidden assumptions, recursions, and GoTo statement
C. Programmers should implement high-consequence functions in minimum required lines of code and follow proper coding standards.
D. Processes should have multiple entry and exit points.

Answer: ABC

Explanation:
The various coding practices that are helpful in simplifying the code are as follows: Programmers should implement high-consequence functions in minimum required lines of code and follow the proper coding standards. Software should implement the functions that are defined in the software specification. Software should avoid ambiguities and hidden assumptions, recursion, and GoTo statements. Programmers should use multiple small and simple functions rather than a complex function. The processes should have only one entry point and minimum exit points. Interdependencies should be minimum so that a process module or component can be disabled when it is not needed, or replaced when it is found insecure or a better alternative is available, without disturbing the software operations. Programmers should use object-oriented techniques to keep the code simple and small. Some of the object-oriented techniques are object inheritance, encapsulation, and polymorphism. Answer D is incorrect. Processes should have only one entry point and the minimum number of exit points.

NEW QUESTION 4
Which of the following testing methods verifies the interfaces between components against a software design?

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

Answer: B

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

be sure that all existent paths are tested.

NEW QUESTION 5
What component of the change management system is responsible for evaluating, testing, and documenting changes created to the project scope?

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

Answer: C

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

NEW QUESTION 6
The service-oriented modeling framework (SOMF) provides a common modeling notation to address alignment between business and IT organizations. Which of the following principles does the SOMF concentrate on? Each correct answer represents a part of the solution. Choose all that apply.

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

Answer: ABCE

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

NEW QUESTION 7
Which of the following are the types of access controls? Each correct answer represents a complete solution. Choose three.

A. Physical
B. Technical
C. Administrative
D. Automatic

Answer: ABC

Explanation:
Security guards, locks on the gates, and alarms come under physical access control. Policies and procedures implemented by an organization come under administrative access control. IDS systems, encryption, network segmentation, and antivirus controls come under technical access control. Answer D is incorrect. There is no such type of access control as automatic control.

NEW QUESTION 8
Which of the following processes culminates in an agreement between key players that a system in its current configuration and operation provides adequate protection controls?

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

Answer: C

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

NEW QUESTION 9
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
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 10
Which of the following are examples of the application programming interface (API)? Each correct answer represents a complete solution. Choose three.

A. HTML
B. PHP
C. .NET
D. Perl

Answer: BCD

Explanation:
Perl, .NET, and PHP are examples of the application programming interface (API). API is a set of routines, protocols, and tools that users can use to work with a component, application, or operating system. It consists of one or more DLLs that provide specific functionality. API helps in reducing the development time of applications by reducing application code. Most operating environments, such as MS-Windows, provide an API so that programmers can write applications consistent with the operating environment. Answer A is incorrect. HTML stands for Hypertext Markup Language. It is a set of markup symbols or codes used to create Web pages and define formatting specifications. The markup tells the Web browser how to display the content of the Web page.

NEW QUESTION 15
Which of the following types of signatures is used in an Intrusion Detection System to trigger on attacks that attempt to reduce the level of a resource or system, or to cause it to crash?

A. Access
B. Benign
C. DoS
D. Reconnaissance

Answer: C

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

NEW QUESTION 19

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

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

Answer: B

Explanation:
Configuration identification is known as the decomposition process of a verification system into Configuration Items. Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined. Baselining an attribute forces formal configuration change control processes to be effected in the event that these attributes are changed. Answer D is incorrect. Configuration control is a procedure of the Configuration management. Configuration control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them. It supports the change of the functional and physical attributes of software at various points in time, and performs systematic control of changes to the identified attributes. Configuration control is a means of ensuring that system changes are approved before being implemented. Only the proposed and approved changes are implemented, and the implementation is complete and accurate. Answer A is incorrect. The configuration status accounting procedure is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time. It supports the functional and physical attributes of software at various points in time, and performs systematic control of accounting to the identified attributes for the purpose of maintaining software integrity and traceability throughout the software development life cycle. Answer C is incorrect. Configuration auditing is the quality assurance element of configuration management. It is occupied in the process of periodic checks to establish the consistency
and completeness of accounting information and to validate that all configuration management policies are being followed. Configuration audits are broken into functional and physical configuration audits. They occur either at delivery or at the moment of effecting the change. A functional configuration audit ensures that functional and performance attributes of a configuration item are achieved, while a physical configuration audit ensures that a configuration item is installed in accordance with the requirements of its detailed design documentation.

NEW QUESTION 21
You have a storage media with some data and you make efforts to remove this data. After performing this, you analyze that the data remains present on the media. Which of the following refers to the above mentioned condition?

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

Answer: D

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

NEW QUESTION 26
Which of the following is a name, symbol, or slogan with which a product is identified?

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

Answer: A

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

NEW QUESTION 28
Della works as a security engineer for BlueWell Inc. She wants to establish configuration management and control procedures that will document proposed or actual changes to the information system. Which of the following phases of NIST SP 800-37 C&A methodology will define the above task?

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

Answer: C

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

NEW QUESTION 31
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 34
Which of the following elements of BCP process includes the areas of plan implementation, plan testing, and ongoing plan maintenance, and also involves defining and documenting the continuity strategy?

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

Answer: A

Explanation:
The business continuity plan development refers to the utilization of the information collected in the Business Impact Analysis (BIA) for the creation of the recovery strategy plan to support the critical business functions. The information gathered from the BIA is mapped out to make a strategy for creating a continuity plan. The business continuity plan development process includes the areas of plan implementation, plan testing, and ongoing plan maintenance. This phase also consists of defining and documenting the continuity strategy. Answer C is incorrect. The scope and plan initiation process in BCP symbolizes the beginning of the BCP process. It emphasizes on creating the scope and the additional elements required to define the parameters of the plan. The scope and plan initiation phase embodies a check of the company's operations and support services. The scope activities include creating a detailed account of the work required, listing the resources to be used, and defining the management practices to be employed. Answer B is incorrect. The business impact assessment is a method used to facilitate business units to understand the impact of a disruptive event. This phase includes the execution of a vulnerability assessment. This process makes out the mission-critical areas and business processes that are important for the survival of business. It is similar to the risk assessment process. The function of a business impact assessment process is to create a document, which is used to help and understand what impact a disruptive event would have on the business. Answer D is incorrect. The plan approval and implementation process involves creating enterprise-wide awareness of the plan, getting the final senior management signoff, and implementing a maintenance procedure for updating the plan as required.

NEW QUESTION 37
Software Development Life Cycle (SDLC) is a logical process used by programmers to develop software. Which of the following SDLC phases meets the audit objectives defined below: System and data are validated. System meets all user requirements. System meets all control requirements.

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

Answer: A

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

NEW QUESTION 42
Which of the following techniques is used to identify attacks originating from a botnet?

A. Passive OS fingerprinting
B. Recipient filtering
C. IFilter
D. BPF-based filter

Answer: A

Explanation:
Passive OS fingerprinting can identify attacks originating from a botnet. Network Administrators can configure the firewall to take action on a botnet attack by

using information obtained from passive OS fingerprinting. Passive OS fingerprinting (POSFP) allows the sensor to determine the operating system used by the hosts. The sensor examines the traffic flow between two hosts and then stores the operating system of those two hosts along with their IP addresses. In order to determine the type of operating system, the sensor analyzes TCP SYN and SYN ACK packets that are traveled on the network. The sensor computes the attack relevance rating to determine the relevancy of victim attack using the target host OS. After it, the sensor modifies the alert's risk rating or filters the alert for the attack. Passive OS fingerprinting is also used to improve the alert output by reporting some information, such as victim OS, relevancy to the victim in the alert, and source of the OS identification. Answer D is incorrect. A BPF-based filter is used to limit the number of packets seen by tcpdump; this renders the output more usable on networks with a high volume of traffic. Answer B is incorrect. Recipient filtering is used to block messages on the basis of whom they are sent to. Answer C is incorrect. IFilters are used to extract contents from files that are crawled. IFilters also remove application-specific formatting before the content of a document is indexed by the search engine.

NEW QUESTION 45
What project management plan is most likely to direct the quantitative risk analysis process for a project in a matrix environment?

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

Answer: C

Explanation:
The risk management plan defines how risks will be identified, analyzed, responded to, and then monitored and controlled regardless of the structure of the organization. Answer D is incorrect. The human resources management plan does define how risks will be analyzed. Answer B is incorrect. The staffing management plan does define how risks will be analyzed. Answer A is incorrect. The risk analysis plan does define how risks will be analyzed.

NEW QUESTION 50
Which of the following techniques is used when a system performs the penetration testing with the objective of accessing unauthorized information residing inside a computer?

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

Answer: C

Explanation:
Port scanning identifies open doors to a computer. Hackers and crackers use this technique to obtain unauthorized information.
Port scanning is the first basic step to get the details of open ports on the target system. Port scanning is used to find a hackable server with a hole or vulnerability. A port is a medium of communication between two computers. Every service on a host is identified by a unique 16-bit number called a port. A port scanner is a piece of software designed to search a network host for open ports. This is often used by administrators to check the security of their networks and by hackers to identify running services on a host with the view to compromising it. Port scanning is used to find the open ports, so that it is possible to search exploits related to that service and application. Answer D is incorrect. Phreaking is a process used to crack the phone system. The main aim of phreaking is to avoid paying for long-distance calls. As telephone networks have become computerized, phreaking has become closely linked with computer hacking. This is sometimes called the H/P culture (with H standing for Hacking and P standing for Phreaking). Answer A is incorrect. It is defined as a system using a physical attribute for authenticating. Only authorized users are provided access to network or application. Answer B is incorrect. It is described as a form of eavesdropping in which special equipments are used to pick up the telecommunication signals or data within a computer device.

NEW QUESTION 51
You work as a security manager for BlueWell Inc. You are going through the NIST SP 800- 37 C&A methodology, which is based on four well defined phases. In which of the following phases of NIST SP 800-37 C&A methodology does the security categorization occur?

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

Answer: D

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

NEW QUESTION 52
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 57
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 61
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 66
Which of the following security models dictates that subjects can only access objects through applications?

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

Answer: C

Explanation:
The Clark-Wilson security model dictates that subjects can only access objects through applications. Answer A is incorrect. The Biba model does not let subjects write to objects at a higher integrity level. Answer B is incorrect. The Bell-LaPadula model has a simple security rule, which means a subject cannot read data from a higher level. Answer D is incorrect. There is no such model as Biba-Clark model.

NEW QUESTION 69
Which of the following are the scanning methods used in penetration testing? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABD

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

NEW QUESTION 71
Which of the following features of SIEM products is used in analysis for identifying potential problems and reviewing all available data that are associated with the problems?

A. Security knowledge base
B. Graphical user interface
C. Asset information storage and correlation
D. Incident tracking and reporting

Answer: B

Explanation:
SIEM product has a graphical user interface (GUI) which is used in analysis for identifying potential problems and reviewing all available data that are associated with the problems. A graphical user interface (GUI) is a type of user interface that allows people to interact with programs in more ways than typing commands on computers. The term came into existence because the first interactive user interfaces to computers were not graphical; they were text- and-keyboard oriented and usually consisted of commands a user had to remember and computer responses that were infamously brief. A GUI offers graphical icons, and visual indicators, as opposed to text-based interfaces, typed command labels or text navigation to fully represent the information and actions available to a user. The actions are usually performed through direct manipulation of the graphical elements.

NEW QUESTION 75
Which of the following vulnerabilities occurs when an application directly uses or concatenates potentially hostile input with data file or stream functions?

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

Answer: B

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

NEW QUESTION 76
Which of the following is the process of finding weaknesses in cryptographic algorithms and obtaining the plaintext or key from the ciphertext?

A. Cryptographer
B. Cryptography
C. Kerberos
D. Cryptanalysis

Answer: D

Explanation:
Cryptanalysis is the process of analyzing cipher text and finding weaknesses in cryptographic algorithms. These weaknesses can be used to decipher the cipher text without knowing the secret key. Answer B is incorrect. Kerberos is an industry standard authentication protocol used to verify user or host identity. Kerberos v5 authentication protocol is the default authentication service for Windows 2000. It is integrated into the administrative and security model, and provides secure communication between Windows 2000 Server domains and clients. Answer A is incorrect. A cryptographer is a person who is involved in cryptography.
Answer B is incorrect. Cryptography is a branch of computer science and mathematics. It is used for protecting information by encoding it into an unreadable format known as cipher text.

NEW QUESTION 81
An attacker exploits actual code of an application and uses a security hole to carry out an attack before the application vendor knows about the vulnerability. Which of the following types of attack is this?

A. Replay
B. Zero-day
C. Man-in-the-middle
D. Denial-of-Service

Answer: B

Explanation:
A zero-day attack, also known as zero-hour attack, is a computer threat that tries to exploit computer application vulnerabilities which are unknown to others, undisclosed to the software vendor, or for which no security fix is available. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software vendor knows about the vulnerability. User awareness training is the most effective technique to mitigate such attacks. Answer A is incorrect. A replay attack is a type of attack in which attackers capture packets containing passwords or digital signatures whenever packets pass between two hosts on a network. In an attempt to obtain an authenticated connection, the attackers then resend the captured packet to the system. In this type of attack, the attacker does not know the actual password, but can simply replay the captured packet. Answer B is incorrect. Man-in-the-middle attacks occur when an attacker successfully inserts an intermediary software or program between two communicating hosts. The intermediary software or program allows attackers to listen to and modify the communication packets passing between the two hosts. The software intercepts the communication packets and then sends the information to the receiving host. The receiving host responds to the software, presuming it to be the legitimate client. Answer D is incorrect. A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as network saturation attack or bandwidth consumption attack. Attackers perform DoS attacks by sending a large number of protocol packets to a network.

NEW QUESTION 86
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 88
System Authorization is the risk management process. System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. What are the different phases of System Authorization Plan? Each correct answer represents a part of the solution. Choose all that apply.

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

Answer: BCDE

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

NEW QUESTION 91
Which of the following is a standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system?

A. FITSAF
B. FIPS
C. TCSEC
D. SSAA

Answer: C

Explanation:
Trusted Computer System Evaluation Criteria (TCSEC) is a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. TCSEC was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information. It was replaced with the development of the Common Criteria international standard originally published in 2005. The TCSEC, frequently referred to as the Orange Book, is the centerpiece of the
DoD Rainbow Series publications. Answer D is incorrect. System Security Authorization Agreement (SSAA) is an information security document used in the United States Department of Defense (DoD) to describe and accredit networks and systems. The SSAA is part of the Department of Defense Information Technology Security Certification and Accreditation Process, or DITSCAP (superseded by DIACAP). The DoD instruction (issues in December 1997, that describes DITSCAP and provides an outline for the SSAA document is DODI 5200.40. The DITSCAP application manual (DoD 8510.1- M), published in July 2000, provides additional details. Answer A is incorrect. FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. It provides an approach for federal agencies. It determines how federal agencies are meeting existing policy and establish goals. The main advantage of FITSAF is that it addresses the requirements of Office of Management and Budget (OMB). It also addresses the guidelines provided by the National Institute of Standards and Technology (NIsT). Answer B is incorrect. The Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States federal government for use by all non-military government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community (ANSI, IEEE, ISO, etc.). Some FIPS standards were originally developed by the U.S. government. For instance, standards for encoding data (e.g., country codes), but more significantly some encryption standards, such as the Data Encryption Standard (FIPS 46-3) and the Advanced Encryption Standard (FIPS 197). In 1994, NOAA (Noaa) began broadcasting coded signals called FIPS (Federal Information Processing System) codes along with their standard weather broadcasts from local stations. These codes identify the type of emergency and the specific geographic area (such as a county) affected by the emergency.

NEW QUESTION 95
Which of the following phases of the DITSCAP C&A process is used to define the C&A level of effort, to identify the main C&A roles and responsibilities, and to

create an agreement on the method for implementing the security requirements?

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

Answer: A

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

NEW QUESTION 99
The Data and Analysis Center for Software (DACS) specifies three general principles for software assurance which work as a framework in order to categorize various secure design principles. Which of the following principles and practices does the General Principle 1 include? Each correct answer represents a complete solution. Choose two.

A. Principle of separation of privileges, duties, and roles
B. Assume environment data is not trustworthy
C. Simplify the design
D. Principle of least privilege

Answer: AD

Explanation:
General Principle 1- Minimize the number of high-consequence targets includes the following principles and practices:
Principle of least privilege Principle of separation of privileges, duties, and roles Principle of separation of domains Answer B is incorrect. Assume environment data is not trustworthy principle is included in the General Principle 2. Answer B is incorrect. Simplify the design principle is included in the General Principle 3.

NEW QUESTION 100
Billy is the project manager of the HAR Project and is in month six of the project. The project is scheduled to last for 18 months. Management asks Billy how often the project team is participating in risk reassessment in this project. What should Billy tell management if he's following the best practices for risk management?

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

Answer: D

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

NEW QUESTION 104
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 105
Which of the following sections come under the ISO/IEC 27002 standard?

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

Answer: ABD

Explanation:
ISO/IEC 27002 is an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical

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

NEW QUESTION 109
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 111
Which of the following are the principle duties performed by the BIOS during POST (power- on-self-test)? Each correct answer represents a part of the solution. Choose all that apply.

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

Answer: ABCDE

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

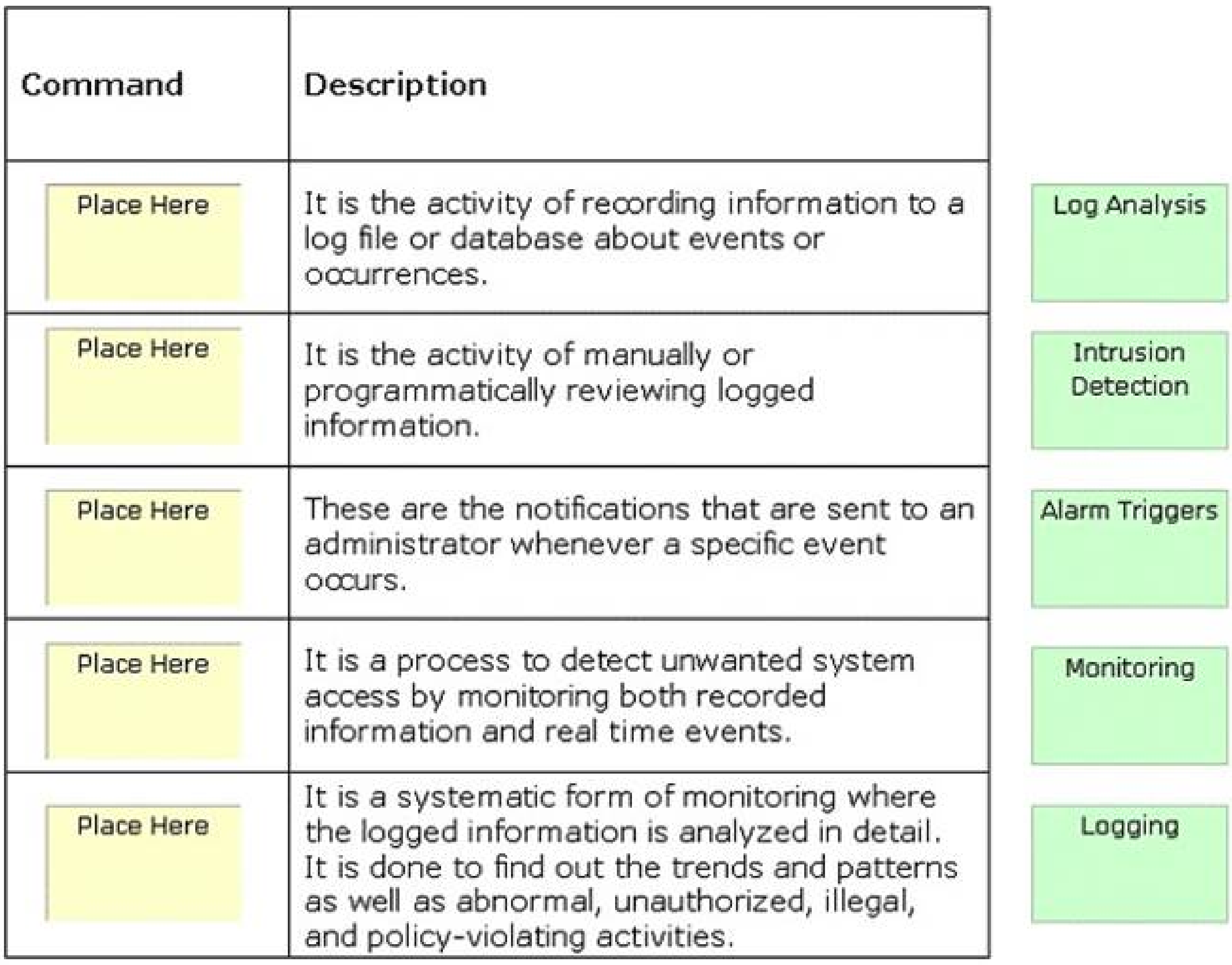
NEW QUESTION 112
Fill in the blank with an appropriate phrase. is used to provide security mechanisms for the storage, processing, and transfer of data.

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 117
DRAG DROP
Auditing is used to track user accounts for file and object access, logon attempts, system shutdown, and many more vulnerabilities to enhance the security of the network. It encompasses a wide variety of activities. Place the different auditing activities in front of their descriptions.



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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 118
Which of the following US Acts emphasized a "risk-based policy for cost-effective security" and makes mandatory for agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget?

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

Answer: A

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

NEW QUESTION 120

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

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

Answer: ACD

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

NEW QUESTION 125
Which of the following models manages the software development process if the developers are limited to go back only one stage to rework?

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

Answer: A

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

NEW QUESTION 130
You work as a system engineer for BlueWell Inc. You want to verify that the build meets its
data requirements, and correctly generates each expected display and report. Which of the following tests will help you to perform the above task?

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

Answer: B

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

NEW QUESTION 133
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 137
How can you calculate the Annualized Loss Expectancy (ALE) that may occur due to a threat?

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

Answer: A

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

NEW QUESTION 141
Which of the following specifies the behaviors of the DRM implementation and any applications that are accessing the implementation?

A. OS fingerprinting
B. OTA provisioning
C. Access control
D. Compliance rule

Answer: D

Explanation:
The Compliance rule specifies the behaviors of the DRM implementation and any 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 Answer B is incorrect. Over- the- air provisioning is a mechanism to deploy MIDlet suites over a network. It is a method of distributing MIDlet suites. MIDlet suite providers install their MIDlet suites on Web servers and provide a hypertext link for downloading. A user can use this link to download the MIDlet suite either through the Internet microbrowser or through WAP on his device. Answer B is incorrect. An access control is a system, which enables an authority to control access to areas and resources in a given physical facility, or computer-based information system. Access control system, within the field of physical security, is generally seen as the second layer in the security of a physical structure. It refers to all mechanisms that control visibility of screens, views, and data within Siebel Business Applications. Answer A is incorrect. OS fingerprinting is a process in which an external host sends special traffic on the external network interface of a computer to determine the computer's operating system. It is one of the primary steps taken by hackers in preparing an attack.

NEW QUESTION 143
Information Security management is a process of defining the security controls in order to protect information assets. The first action of a management program to implement information security is to have a security program in place. What are the objectives of a security program? Each correct answer represents a complete solution. Choose all that apply.

A. Security education
B. Security organization
C. System classification
D. Information classification

Answer: ABD

Explanation:
The first action of a management program to implement information security is to have a security program in place. The objectives of a security program are as follows: Protect the company and its assets Manage risks by identifying assets, discovering threats, and estimating the risk Provide direction for security activities by framing of information security policies, procedures, standards, guidelines and baselines Information classification Security organization Security education Answer B is incorrect. System classification is not one of the objectives of a security program.

NEW QUESTION 147
Certification and Accreditation (C&A or CnA) is a process for implementing information security. Which of the following is the correct order of C&A phases in a DITSCAP assessment?

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

Answer: C

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

NEW QUESTION 148
Copyright holders, content providers, and manufacturers use digital rights management (DRM) in order to limit usage of digital media and devices. Which of the following security challenges does DRM include? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ACD

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

NEW QUESTION 150
The DARPA paper defines various procedural patterns to perform secure system development practices. Which of the following patterns does it include? Each correct answer represents a complete solution. Choose three.

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

Answer: BCD

Explanation:
The following procedural patterns are defined by the DARPA paper in order to perform secure software development practices: Build the server from the ground up: It includes the following features: Build the server from the ground up. Identify the default installation of the operating system and applications. Support hardening procedures to remove unnecessary services. Identify a vulnerable service for ongoing risk management. Choose the right stuff: It defines guidelines to select right commercial off-the-shelf (COTS) components and decide whether to use and build custom components. Document the server configuration: It supports the creation of an initial configuration baseline and tracks all modifications made to servers and application configurations.
Patch proactively: It supports in applying patches as soon as they are available rather than waiting until the systems cooperate. Red team the design: It supports an independent security assessment from the perspective of an attacker in the quality assurance or testing stage. An independent security assessment is helpful in addressing a security issue before it occurs. Answer A is incorrect. Hidden implementation pattern is not defined in the DARPA paper. This pattern is applicable to software assurance in general. Hidden implementation limits the ability of an attacker to distinguish the internal workings of an application. Answer E is incorrect. Password propagation is not defined in the DARPA paper. This pattern is applicable to aspects of authentication in a Web application. Password propagation provides an alternative by requiring that a user's authentication credentials be verified by the database before providing access to that user's data.

NEW QUESTION 151
Which of the following plans is documented and organized for emergency response, backup operations, and recovery maintained by an activity as part of its security program that will ensure the availability of critical resources and facilitates the continuity of operations in an emergency situation?

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

Answer: C

Explanation:
Contingency plan is prepared and documented for emergency response, backup operations, and recovery maintained by an activity as the element of its security program that will ensure the availability of critical resources and facilitates the continuity of operations in an emergency situation. A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and "triggers" for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption.
Answer D is incorrect. A disaster recovery plan should contain data, hardware, and software that can be critical for a business. It should also include the plan for sudden loss such as hard disc crash. The business should use backup and data recovery utilities to limit the loss of datAnswer 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. Answer B is incorrect. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan.

NEW QUESTION 154
Which of the following configuration management system processes keeps track of the changes so that the latest acceptable configuration specifications are readily available?

A. Configuration Control
B. Configuration Status and Accounting
C. Configuration Verification and Audit
D. Configuration Identification

Answer: B

Explanation:

The configuration status accounting procedure is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time. It supports the functional and physical attributes of software at various points in time, and performs systematic control of accounting to the identified attributes for the purpose of maintaining software integrity and traceability throughout the software development life cycle. The configuration status and accounting process keeps track of the changes so that the latest acceptable configuration specifications are readily available. Answer B is incorrect. The verification and audit processes seek to establish a high level of confidence in how well the Configuration Management activity is working. Answer A 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 D is incorrect. Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined. Baselining an attribute forces formal configuration change control processes to be effected in the event that these attributes are changed.

NEW QUESTION 159
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 164
What are the differences between managed and unmanaged code technologies? Each correct answer represents a complete solution. Choose two.

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

Answer: CD

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

NEW QUESTION 169
Which of the following processes does the decomposition and definition sequence of the Vee model include? Each correct answer represents a part of the solution. Choose all that apply.

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

Answer: BCD

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

NEW QUESTION 173
Which of the following can be used to accomplish authentication? Each correct answer represents a complete solution. Choose all that apply.

A. Encryption
B. Biometrics
C. Token
D. Password

Answer: BCD

Explanation:
The following can be used to accomplish authentication: 1.Password 2.Biometrics 3.Token A password is a secret word or string of characters that is used for authentication, to prove identity, or gain access to a resource.

NEW QUESTION 175
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully performed the following steps of the pre-attack phase to check the security of the We-are-secure network: Gathering information Determining the network range Identifying active systems Now, he wants to find the open ports and applications running on the network. Which of the following tools will he use to accomplish his task?

A. ARIN
B. APNIC
C. RIPE
D. SuperScan

Answer: D

Explanation:
In such a situation, John will use the SuperScan tool to find the open ports and applications on the We-are-secure network. SuperScan is a TCP/UDP port scanner. It also works as a ping sweeper and hostname resolver. It can ping a given range of IP addresses and resolve the host name of the remote system. The features of SuperScan are as follows: It scans any port range from a built-in list or any given range. It performs ping scans and port scans using any IP range. It modifies the port list and port descriptions using the built in editor. It connects to any discovered open port using user-specified "helper" applications. It has the transmission speed control utility. Answer C, A, and B are incorrect. RIPE, ARIN, and APNIC are the Regional Internet Registries (RIR) that manage, distribute, and register public IP addresses within their respective regions. These can be used as passive tools by an attacker to determine the network range.

NEW QUESTION 179
An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

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

Answer: C

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

NEW QUESTION 180
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 185
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 188
FIPS 199 defines the three levels of potential impact on organizations: low, moderate, and high. Which of the following are the effects of loss of confidentiality, integrity, or availability in a high level potential impact?

A. The loss of confidentiality, integrity, or availability might result in a major damage to organizational assets.
B. The loss of confidentiality, integrity, or availability might result in severe damages like life threatening injuries or loss of life.
C. The loss of confidentiality, integrity, or availability might result in major financial losses.
D. The loss of confidentiality, integrity, or availability might cause severe degradation in or loss of mission capability to an extent.

Answer: ABCD

Explanation:
The following are the effects of loss of confidentiality, integrity, or availability in a high level potential impact: It might cause a severe degradation in or loss of mission capability to an extent. It might result in a major damage to organizational assets. It might result in a major financial loss. It might result in severe harms such as serious life threatening injuries or loss of life.

NEW QUESTION 191
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 SOAnswer 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 are the tasks performed by the owner in the information classification schemes? Each correct answer represents a part of the solution. Choose three.

A. To make original determination to decide what level of classification the information requires, which is based on the business requirements for the safety of the data.
B. To review the classification assignments from time to time and make alterations as the business requirements alter.
C. To perform data restoration from the backups whenever required.
D. To delegate the responsibility of the data safeguard duties to the custodian.

Answer: ABD

Explanation:
The different tasks performed by the owner are as follows: He makes the original determination to decide what level of classification the information requires, which is based on the business requirements for the safety of the data. He reviews the classification assignments from time to time and makes alterations as the business needs change. He delegates the responsibility of the data safeguard duties to the custodian. He specifies controls to ensure confidentiality, integrity and availability. Answer B is incorrect. This task is performed by the custodian and not by the owner.

NEW QUESTION 196
What are the various benefits of a software interface according to the "Enhancing the Development Life Cycle to Produce Secure Software" document? Each correct answer represents a complete solution. Choose three.

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

Answer: ABD

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

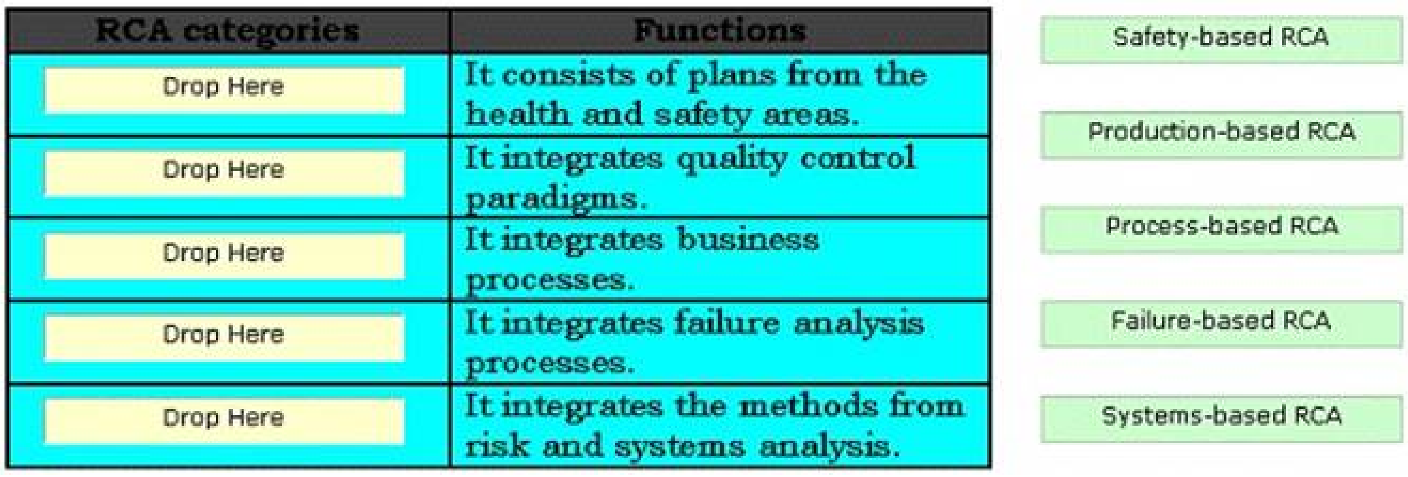
NEW QUESTION 199
You work as a Network Administrator for uCertify Inc. You need to secure web services of your company in order to have secure transactions. Which of the following will you recommend for providing security?

A. SSL
B. VPN
C. S/MIME
D. HTTP

Answer: A

Explanation:
The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. URLs that require an SSL connection start with https: instead of http:. Answer B is incorrect. S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of e- mail encapsulated in MIME. S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity, non-repudiation of origin (using digital signatures), privacy, and data security (using encryption). Answer D is incorrect. Hypertext Transfer Protocol (HTTP) is a client/server TCP/IP protocol used on the World Wide Web (WWW) to display Hypertext Markup Language (HTML) pages. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when a client application or browser sends a request to the server using HTTP commands, the server responds with a message containing the protocol version, success or failure code, server information, and body content, depending on the request. HTTP uses TCP port 80 as the default port. Answer B is incorrect. A Virtual Private Network (VPN) is a computer network that is implemented in an additional software layer (overlay) on top of an existing larger network for the purpose of creating a private scope of computer communications or providing a secure extension of a private network into an insecure network such as the Internet. The links between nodes of a Virtual Private Network are formed over logical connections or virtual circuits between hosts of the larger network. The Link Layer protocols of the virtual network are said to be tunneled through the underlying transport network.

NEW QUESTION 201
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.
Drop Here	It integrates quality control paradigms.
Drop Here	It integrates business processes.
Drop Here	It integrates failure analysis processes.
Drop Here	It integrates the methods from risk and systems analysis.

Safety-based RCA
Production-based RCA
Process-based RCA
Failure-based RCA
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 204
Which of the following are Service Level Agreement (SLA) structures as defined by ITIL? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BDE

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

NEW QUESTION 208
Which of the following classification levels defines the information that, if disclosed to the unauthorized parties, could be reasonably expected to cause exceptionally grave damage to the national security?

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

Answer: D

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

NEW QUESTION 213
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 217
Frank is the project manager of the NHH Project. He is working with the project team to create a plan to document the procedures to manage risks throughout the project. This document will define how risks will be identified and quantified. It will also define how contingency plans will be implemented by the project team. What document is Frank and the NHH Project team creating in this scenario?

A. Risk management plan
B. Project plan
C. Project management plan
D. Resource management plan

Answer: A

Explanation:
The risk management plan, part of the comprehensive management plan, defines how risks will be identified, analyzed, monitored and controlled, and even responded to. 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 B is incorrect. The project management plan is a comprehensive plan that communicates the intent of the project for all project management knowledge areas. Answer B is incorrect. The project plan is not an official PMBOK project management plan. Answer D is incorrect. The resource management plan defines the management of project resources, such as project team members, facilities, equipment, and contractors.

NEW QUESTION 219
John works as a systems engineer for BlueWell Inc. He has modified the software, and wants to retest the application to ensure that bugs have been fixed or not. Which of the following tests should John use to accomplish the task?

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

Answer: D

Explanation:
John should use the regression tests to retest the application to guarantee that bugs have been fixed. This test will help him to check that the earlier working functions have not failed as a result of the changes, and newly added features have not created problems with the previous versions. The various types of internal tests performed on builds are as follows: Regression tests: It is also known as the verification testing. These tests are developed to confirm that capabilities in earlier builds continue to work correctly in the subsequent builds. Functional test: These tests emphasizes on verifying that the build meets its functional and data requirements and correctly generates each expected display and report. Performance tests: These tests are used to identify the performance thresholds of each build. Reliability tests: These tests are used to identify the reliability thresholds of each build.

NEW QUESTION 222
In which of the following testing methods is the test engineer equipped with the knowledge of system and designs test cases or test data based on system knowledge?

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

Answer: D

Explanation:
Graybox testing is a combination of whitebox testing and blackbox testing. In graybox testing, the test engineer is equipped with the knowledge of system and designs test cases or test data based on system knowledge. The security tester typically performs graybox testing to find vulnerabilities in software and network system. Answer B is incorrect. Whitebox testing is a testing technique in which an organization provides full knowledge about the infrastructure to the testing team. The information, provided by the organization, often includes network diagrams, source codes, and IP addressing information of the infrastructure to be tested. Answer A is incorrect. Integration testing is a logical extension of unit testing. It is performed to identify the problems that occur when two or more units are combined into a component. During integration testing, a developer combines two units that have already been tested into a component, and tests the interface between the two units. Although integration testing can be performed in various ways, the following three approaches are generally used: The top-down approach The bottom-up approach The umbrella approach Answer B is incorrect. Regression testing can be performed any time when a program needs to be modified either to add a feature or to fix an error. It is a process of repeating Unit testing and Integration testing whenever existing tests need to be performed again along with the new tests. Regression testing is performed to ensure that no existing errors reappear, and no new errors are introduced.

NEW QUESTION 227
The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum standard process for the certification and accreditation of computer and telecommunications systems that handle U.S. national security information. What are the different types of NIACAP accreditation? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABD

Explanation:
NIACAP accreditation is of three types depending on what is being certified. They are as follows: 1.Site accreditation: This type of accreditation evaluates the applications and systems at a specific, self contained location. 2.Type accreditation: This type of accreditation evaluates an application or system that is distributed to a number of different locations. 3.System accreditation: This accreditation evaluates a major application or general support system. Answer B is incorrect. No such type of NIACAP accreditation exists.

NEW QUESTION 230
Which of the following statements about a host-based intrusion prevention system (HIPS) are true? Each correct answer represents a complete solution. Choose two.

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

Answer: CD

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

NEW QUESTION 231
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 236
Shoulder surfing is a type of in-person attack in which the attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard of an employee's computer while he is typing in his password at any access point such as a terminal/Web site. Which of the following is violated in a shoulder surfing attack?

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

Answer: C

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

NEW QUESTION 241
Which of the following are the types of intellectual property? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABD

Explanation:
Common types of intellectual property include copyrights, trademarks, patents, industrial design rights, and trade secrets. A copyright is a form of intellectual property, which secures to its holder the exclusive right to produce copies of his or her works of original expression, such as a literary work, movie, musical work or sound recording, painting, photograph, computer program, or industrial design, for a defined, yet extendable, period of time. It does not cover ideas or facts. Copyright laws protect intellectual property from misuse by other individuals. A trademark is a distinctive sign used by an individual, business organization, or other legal entity to identify that the products or services to consumers with which the trademark appears originate from a unique source, and to distinguish its products or services from those of other entities. A trademark is designated by the following symbols: : It is for an unregistered trade mark and it is used to promote or brand goods. : It is for an unregistered service mark and it is used to promote or brand services. : It is for a registered trademark. A patent is a set of exclusive rights granted by a state to an inventor or their assignee for a limited period of time in exchange for a public disclosure of an invention. Answer B is incorrect. It is not a type of intellectual property.

NEW QUESTION 242
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 244
A service provider guarantees for end-to-end network traffic performance to a customer. Which of the following types of agreement is this?

A. SLA
B. VPN
C. NDA
D. LA

Answer: A

Explanation:
This is a type of service-level agreement. A service-level agreement (SLA) is a negotiated agreement between two parties where one is the customer and the other is the service provider. It records a common understanding about services, priorities, responsibilities, guarantees, and warranties. Each area of service scope should have the 'level of service' defined. The SLA may specify the levels of availability, serviceability, performance, operation, or other attributes of the service,

such as billing. Answer B is incorrect. Non-disclosure agreements (NDAs) are often used to protect the confidentiality of an invention as it is being evaluated by potential licensees. Answer D is incorrect. License agreements (LA) describe the rights and responsibilities of a party related to the use and exploitation of intellectual property. Answer B is incorrect. There is no such type of agreement as VPN.

NEW QUESTION 245
An assistant from the HR Department calls you to ask the Service Hours & Maintenance Slots for your ERP system. In which document will you most probably find this information?

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

Answer: A

Explanation:
You will most probably find this information in the Service Level Agreement document. Amongst other information, SLA contains information about the agreed Service Hours and maintenance slots for any particular Service. Service Level Agreement
(frequently abbreviated as SLA) is a part of a service contract where the level of service is formally defined. In practice, the term SLA is sometimes used to refer to the contracted delivery time (of the service) or performance. Service Level Agreement (SLA) is a negotiated agreement between two parties where one is the customer and the other is the service provider. This can be a legally binding formal or informal 'contract'. Contracts between the Service Provider and other third parties are often (incorrectly) called SLAs, as the level of service has been set by the (principal) customer there can be no 'agreement' between third parties (these agreements are simply a 'contract'). Operating Level Agreements or OLA(s) however, may be used by internal groups to support SLA (s). Answer B is incorrect. Release Policy is a set of rules for deploying releases into the live operational environment, defining different approaches for releases depending on their urgency and impact. Answer B is incorrect. The Service Level Requirements document contains the requirements for a service from the client viewpoint, defining detailed service level targets, mutual responsibilities, and other requirements specific to a certain group of customers. Answer D is incorrect. Underpinning Contract (UC) is a contract between an IT service provider and a third party. In another way, it is an agreement between the IT organization and an external provider about the delivery of one or more services. The third party provides services that support the delivery of a service to a customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level targets in an SLA.

NEW QUESTION 250
......