CSSLP.exam.220q

Number: CSSLP
Passing Score: 800
Time Limit: 120 min

CSSLP

Certified Secure Software Lifecycle Professional

Sections

1. Volume A
2. Volume B
3. Volume C

Exam A

QUESTION 1
Which of the following DITSCAP C&A phases takes place between the signing of the initial version of the SSAA and the formal accreditation of the system?

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

Correct Answer: D
Section: Volume A

Explanation

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

QUESTION 2
In which of the following testing methodologies do assessors use all available documentation and work under no constraints, and attempt to circumvent the security features of an information system?

A. Full operational test
B. Penetration test
C. Paper test

D. Walk-through test

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

QUESTION 3
You work as a systems engineer for BlueWell Inc. Which of the following tools will you use to look outside your own organization to examine how others achieve their performance levels, and what processes they use to reach those levels?

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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
Explanation: Benchmarking is the tool used by system assessment process to provide a point of reference by which performance measurements can be reviewed with respect to other organizations. Benchmarking is also recognized as Best Practice Benchmarking or Process Benchmarking. It is a process used in management and mostly useful for strategic management. It is the process of comparing the business processes and performance metrics including cost, cycle

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

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

QUESTION 4

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

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

Correct Answer: A
Section: Volume A

Explanation

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

QUESTION 5
The NIST Information Security and Privacy Advisory Board (ISPAB) paper "Perspectives on Cloud Computing and Standards" specifies potential advantages and disdvantages of virtualization. Which of the following disadvantages does it include? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: CDEFG
Section: Volume A
Explanation

Explanation/Reference:
Explanation: The potential security disadvantages of virtualization are as follows: It increases configuration effort because of complexity and composite system. It initiates the problem of how to prevent overlap while mapping VM storage onto host files. It introduces the problem of virtualizing the TPM. It creates the possibility that remote attestation may not work. It initiates the problem of detecting VM covert channels. It involves new protection mechanisms for preventing VM escape, VM detection, and VM-VM interference. It initiates the possibility of virtual networking configuration errors. It initiates the risk that malicious software is targeting the VM environment.
It increases overall security risk shared resources, such as networks, clipboards, clocks, printers, desktop management, and folders. Answer: A and B are incorrect.

These are not the disadvantages of virtualization, as described in the NIST Information Security and Privacy Advisory Board (ISPAB) paper "Perspectives on Cloud Computing and Standards".

QUESTION 6
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

Correct Answer: ABC
Section: Volume A
Explanation
Explanation/Reference:
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.

QUESTION 7
What are the subordinate tasks of the Initiate and Plan IA C&A phase of the DIACAP process? Each correct answer represents a complete solution. Choose all that apply.

A. Initiate IA implementation plan B.
Develop DIACAP strategy
C. Assign IA controls.
D. Assemble DIACAP team
E. Register system with DoD Component IA Program.
F. Conduct validation activity.

Correct Answer: ABCDE
Section: Volume A
Explanation

Explanation/Reference:
Explanation: The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk.

The subordinate tasks of the Initiate and Plan IA C&A phase are as follows: Register system with DoD Component IA Program. Assign IA controls. Assemble DIACAP team. Develop DIACAP strategy. Initiate IA implementation plan. Answer: F is incorrect. Validation activities are conducted in the second phase of the DIACAP process, i.e., Implement and Validate Assigned IA Controls.

QUESTION 8
Which of the following attacks causes software to fail and prevents the intended users from accessing software?

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

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

QUESTION 9
FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls have been implemented?

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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:

Explanation: The following are the five levels of FITSAF based on SEI's Capability Maturity Model (CMM): Level 1: The first level reflects that an asset has documented a security policy. Level 2: The second level shows that the asset has documented procedures and controls to implement the policy. Level 3: The third level indicates that these procedures and controls have been implemented. Level 4: The fourth level shows that the procedures and controls are tested and reviewed. Level 5: The fifth level is the final level and shows that the asset has procedures and controls fully integrated into a comprehensive program.

QUESTION 10
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

Correct Answer: A
Section: Volume A
Explanation
Explanation/Reference:
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.

QUESTION 11
Della work as a project manager for BlueWell Inc. A threat with a dollar value of $250,000 is expected to happen in her project and the frequency of threat occurrence per year is 0.01. What will be the annualized loss expectancy in her project?

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

Correct Answer: B

Section: Volume A
Explanation

Explanation/Reference:
Explanation: The annualized loss expectancy in her project will be $2,500. Annualized loss expectancy (ALE) is the annually expected financial loss to an organization from a threat. The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as follows: ALE = Single Loss Expectancy (SLE) * Annualized Rate of Occurrence (ARO) Here, it is as follows: ALE = SLE * ARO
= 250,000 * 0.01
= 2,500
Answer: D, C, and A are incorrect. These are not valid answers.

QUESTION 12
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 statements.

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.

Correct Answer: ABC
Section: Volume A
Explanation

Explanation/Reference:
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.

QUESTION 13
Which of the following methods does the Java Servlet Specification v2.4 define in the HttpServletRequest interface that control programmatic security? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: BCD
Section: Volume A
Explanation

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

QUESTION 14
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.

Correct Answer: C
Section: Volume A

Explanation

Explanation/Reference:
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 data. Answer: A is incorrect. This is not a valid statement about the qualitative risk analysis data. Answer: B is incorrect. This is not a valid statement about the qualitative risk analysis data.

QUESTION 15
FIPS 199 defines the three levels of potential impact on organizations. Which of the following potential impact levels shows limited adverse effects on organizational operations, organizational assets, or individuals?

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

Correct Answer: B
Section: Volume A
Explanation

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

QUESTION 16
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

Correct Answer: B

Section: Volume A
Explanation

Explanation/Reference:
Explanation: Configuration identification is known as the decomposition process of a verification system into Configuration Items. Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an enduser 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.

QUESTION 17
Bill is the project manager of the JKH Project. He and the project team have identified a risk event in the project with a high probability of occurrence and the risk event has a high cost impact on the project. Bill discusses the risk event with Virginia, the primary project customer, and she decides that the requirements surrounding the risk event should be removed from the project. The removal of the requirements does affect the project scope, but it can release the project from the high risk exposure. What risk response has been enacted in this project?

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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
Explanation: This is an example of the avoidance risk response. Because the project plan has been changed to avoid the risk event, so it is considered the avoidance risk response. Risk avoidance is a technique used for threats. It creates changes to the project management plan that are meant to either eliminate the

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

QUESTION 18
Martha registers a domain named Microsoft.in. She tries to sell it to Microsoft Corporation. The infringement of which of the following has she made?

A. Copyright
B. Trademark
C. Patent
D. Intellectual property

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
Explanation: According to the Lanham Act, domain names fall under trademarks law. A new section 43(d) of the Trademark Act (Lanham Act) states that anyone who in bad faith registers, traffics in, or uses a domain name that infringes or dilutes another's trademark has committed trademark infringement. Factors involved in assessing bad faith focus on activities typically associated with cyberpiracy or cybersquatting, such as whether the registrant has offered to sell the domain name to the trademark holder for financial gain without having used or intended to use it for a bona fide business; whether the domain-name registrant registered multiple domain names that are confusingly similar to the trademarks of others; and whether the trademark incorporated in the domain name is distinctive and famous. Other factors are whether the domain name consists of the legal name or common handle of the domain-name registrant and whether the domain-name registrant previously used the mark in connection with a bona fide business.

QUESTION 19
Which of the following is a variant with regard to Configuration Management?

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

Correct Answer: C
Section: Volume A

Explanation

Explanation/Reference:
Explanation: A CI that has the same essential functionality as another CI but a bit different in some small manner, and therefore, might be required to be analyzed along with its generic group. A Configuration item (CI) is an IT asset or a combination of IT assets that may depend and have relationships with other IT processes. A CI will have attributes which may be hierarchical and relationships that will be assigned by the configuration manager in the CM database. The Configuration Item
(CI) attributes are as follows: 1.Technical: It is data that describes the CI's capabilities which include software version and model numbers, hardware and manufacturer specifications, and other technical details like networking speeds, and data storage size. Keyboards, mice and cables are considered consumables. 2.Ownership: It is part of financial asset management, ownership attributes, warranty, location, and responsible person for the CI. 3.Relationship: It is the relationship among hardware items, software, and users. Answer: B, D, and A are incorrect. These are incorrect definitions of a variant with regard to Configuration Management.

QUESTION 20
The organization level is the Tier 1 and it addresses risks from an organizational perspective. What are the various Tier 1 activities? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: ABC
Section: Volume A
Explanation

Explanation/Reference:
Explanation: The Organization Level is the Tier 1, and it addresses risks from an organizational perspective. It includes the following points: The techniques and methodologies an organization plans to employ, to evaluate information system-related security risks. During risk assessment, the methods and procedures the organization plans to use, to evaluate the significance of the risks identified. The types and extent of risk mitigation measures the organization plans to employ, to address identified risks. The level of risk tolerance. According to the environment of operation, how the organization plans to monitor risks on an ongoing basis, given the inevitable changes to organizational information system.
The organization plans to use the degree and type of oversight, in order to ensure that the risk management strategy is being effectively carried out.Answer: D is incorrect. The RMF primarily operates at Tier 3.

QUESTION 21
An asset with a value of $600,000 is subject to a successful malicious attack threat twice a year. The asset has an exposure of 30 percent to the threat. What will be the annualized loss expectancy?

A. $360,000 B.
$180,000
C. $280,000
D. $540,000

Correct Answer: A
Section: Volume A

Explanation

Explanation/Reference:
Explanation: The annualized loss expectancy will be $360,000. Annualized loss expectancy (ALE) is the annually expected financial loss to an organization from a threat. The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as follows:

ALE = Single Loss Expectancy (SLE) * Annualized Rate of Occurrence (ARO)
Here, it is as follows:
SLE = Asset value * EF (Exposure factor)
= 600,000 * (30/100)
= 600,000 * 0.30
= 180,000
ALE = SLE * ARO
= 180,000 * 2
= 360,000
Answer: C, B, and D are incorrect. These are not valid answers.

QUESTION 22
Which of the following are the common roles with regard to data in an information classification program? Each correct answer represents a complete solution. Choose all that apply.

A. Editor
B. Custodian
C. Owner
D. User

E. Security auditor

Correct Answer: BCDE
Section: Volume A
Explanation

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

QUESTION 23
Which of the following life cycle modeling activities establishes service relationships and message exchange paths?

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

Correct Answer: A
Section: Volume A

Explanation

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

QUESTION 24
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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
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.

QUESTION 25
Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. Which of the following statements are true about Certification and Accreditation? Each correct answer represents a complete solution. Choose two.

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

Correct Answer: AC

Section: Volume A
Explanation

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

QUESTION 26
The Phase 1 of DITSCAP C&A is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. What are the process activities of this phase? Each correct answer represents a complete solution. Choose all that apply.

A. Negotiation
B. Registration
C. Document mission need
D. Initial Certification Analysis

Correct Answer: ABC
Section: Volume A
Explanation

Explanation/Reference:
Explanation: The Phase 1 of DITSCAP C&A is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. The Phase 1 starts with the input of the mission need. This phase comprises three process activities: Document mission need Registration Negotiation Answer: D is incorrect. Initial Certification Analysis is a Phase 2 activity.

QUESTION 27
Which of the following NIST Special Publication documents provides a guideline on network security testing?

A. NIST SP 800-42
B. NIST SP 800-53A
C. NIST SP 800-60 D. NIST SP 800-53

E. NIST SP 800-37
F. NIST SP 800-59

Correct Answer: A
Section: Volume A
Explanation

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

QUESTION 28
Which of the following tools is used to attack the Digital Watermarking?

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

Correct Answer: C
Section: Volume A

Explanation

Explanation/Reference:
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.

QUESTION 29

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

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

Correct Answer: B
Section: Volume A
Explanation

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

QUESTION 30
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

Correct Answer: C
Section: Volume A

Explanation

Explanation/Reference:
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.

QUESTION 31
You work as a project manager for BlueWell Inc. You with your team are using a method or a (technical) process that conceives the risks even if all theoretically possible safety measures would be applied. One of your team member wants to know that what is a residual risk. What will you reply to your team member?

A. It is a risk that remains because no risk response is taken.

B. It is a risk that can not be addressed by a risk response.
C. It is a risk that will remain no matter what type of risk response is offered.
D. It is a risk that remains after planned risk responses are taken.

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
Explanation: Residual risks are generally smaller risks that remain in the project after larger risks have been addressed. The residual risk is the risk or danger of an action or an event, a method or a (technical) process that still conceives these dangers even if all theoretically possible safety measures would be applied. The formula to calculate residual risk is (inherent risk) x (control risk) where inherent risk is (threats vulnerability). Answer: B is incorrect. This is not a valid statement about residual risks. Answer: C is incorrect. This is not a valid statement about residual risks. Answer: A is incorrect. This is not a valid statement about residual risks.

QUESTION 32
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

Correct Answer: A
Section: Volume A

Explanation

Explanation/Reference:
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.

QUESTION 33
Which of the following statements is true about residual risks?

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

Correct Answer: A
Section: Volume A

Explanation

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

QUESTION 34
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

Correct Answer: C
Section: Volume A

Explanation

Explanation/Reference:

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.

QUESTION 35
Which of the following statements best describes the difference between the role of a data owner and the role of a data custodian?

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

Correct Answer: D
Section: Volume A
Explanation

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

QUESTION 36
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

Correct Answer: C
Section: Volume A

Explanation

Explanation/Reference:
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.

QUESTION 37
Which of the following secure coding principles and practices defines the appearance of code listing so that a code reviewer and maintainer who have not written that code can easily understand it?

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

Correct Answer: C
Section: Volume A

Explanation

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

QUESTION 38
Which of the following software review processes increases the software security by removing the common vulnerabilities, such as format string exploits, race conditions, memory leaks, and buffer overflows?

A. Management review
B. Code review
C. Peer review
D. Software audit review

Correct Answer: B

Section: Volume A
Explanation

Explanation/Reference:
Explanation: A code review is a systematic examination of computer source code, which searches and resolves issues occurred in the initial development phase. It increases the software security by removing common vulnerabilities, such as format string exploits, race conditions, memory leaks, and buffer overflows. A code review is performed in the following forms: Pair programming Informal walkthrough Formal inspection Answer: C is incorrect. A peer review is an examination process in which author and one or more colleagues examine a work product, such as document, code, etc., and evaluate technical content and quality. According to the Capability Maturity Model, peer review offers a systematic engineering practice in order to detect and resolve issues occurring in the software artifacts, and stops the leakage into field operations. Answer: A is incorrect. Management review is a management study into a project's status and allocation of resources. Answer: D is incorrect. In software audit review one or more auditors, who are not members of the software development organization, perform an independent examination of a software product, software process, or a set of software processes for assessing compliance with specifications, standards, contractual agreements, or other specifications.

QUESTION 39
Which of the following governance bodies directs and coordinates implementations of the information security program?

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

Correct Answer: A
Section: Volume A

Explanation

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

Governance Body	Membership	Responsibilities
Information Security Steering Commitee	CFO, CEO, COO, CTO, VP Business units chaired by CISO	It establishes and supports security programs
Senior Management	C-level, unit VPs and senior VPs	It provides management, operational and technical controls to satisfy security requirements.
Chief Information Security Officer	CISO and staff	It directs and coordinates implementations of information security program.
Business Unit Managers	Department heads and supervisors	They Classify and establish requirements for safeguarding information assets.

QUESTION 40
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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
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.

QUESTION 41
Which of the following methods offers a number of modeling practices and disciplines that contribute to a successful service-oriented life cycle management and modeling?

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

Correct Answer: A
Section: Volume A

Explanation

Explanation/Reference:
Explanation: The service-oriented modeling framework (SOMF) has been proposed by author Michael Bell as a service-oriented modeling language for software development that employs disciplines and a holistic language to provide strategic solutions to enterprise problems. The service-oriented modeling framework (SOMF) is a service-oriented development life cycle methodology. It offers a number of modeling practices and disciplines that contribute to a successful serviceoriented life cycle management and modeling. The service-oriented modeling framework illustrates the major elements that identify the "what to do" aspects of a service development scheme. Answer: B is incorrect. The service-oriented architecture (SOA) is a flexible set of design principles used during the phases of systems development and integration. Answer: D is incorrect. The service-oriented modeling and architecture (SOMA) includes an analysis and design method that extends traditional object-oriented and component-based analysis and design methods to include concerns relevant to and supporting SOA. Answer: C is incorrect. SABSA (Sherwood Applied Business Security Architecture) is a framework and methodology for Enterprise Security Architecture and Service Management. It is a model and a methodology for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives.

QUESTION 42
Which of the following phases of DITSCAP includes the activities that are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle?

A. Phase 3, Validation
B. Phase 1, Definition
C. Phase 2, Verification

D. Phase 4, Post Accreditation Phase

Correct Answer: D
Section: Volume A
Explanation

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

QUESTION 43
Joseph works as a Software Developer for WebTech Inc. He wants to protect the algorithms and the techniques of programming that he uses in developing an application. Which of the following laws are used to protect a part of software?

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

Correct Answer: B
Section: Volume A
Explanation

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

QUESTION 44
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

Correct Answer: C
Section: Volume A

Explanation

Explanation/Reference:
Explanation: Following are the basic categories of signatures: Informational (benign): These types of signatures trigger on normal network activity. For example: ICMP echo requests The opening or closing of TCP or UDP connections Reconnaissance: These types of signatures trigger on attacks that uncover resources and hosts that are reachable, as well as any possible vulnerabilities that they might contain. For example: Reconnaissance attacks include ping sweeps DNS queries Port scanning Access: These types of signatures trigger on access attacks, which include unauthorized access, unauthorized escalation of privileges, and access to protected or sensitive data. For example:

Back Orifice A Unicode attack against the Microsoft IIS NetBus DoS: These types of signatures trigger on attacks that attempt to reduce the level of a resource or system, or to cause it to crash. For example: TCP SYN floods The Ping of Death Smurf Fraggle Trinoo Tribe Flood Network

QUESTION 45
Which of the following is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention?

A. Copyright
B. Snooping
C. Utility model
D. Patent

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
Explanation: A patent is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention. Answer: A is incorrect. A copyright is a form of intellectual property, which secures to its holder the exclusive right to produce copies of his or her works of original expression, such as a literary work, movie, musical work or sound recording, painting, photograph, computer program, or industrial design, for a defined, yet extendable, period of time. It does not cover ideas or facts. Copyright laws protect intellectual property from misuse by other individuals. Answer: B is incorrect. Snooping is an activity of observing the content that appears on a computer monitor or watching what a user is typing. Snooping also occurs by using software programs to remotely monitor activity on a computer or network device. Hackers or attackers use snooping techniques and equipment such as keyloggers to monitor keystrokes, capture passwords and login information, and to intercept e-mail and other private communications. Sometimes, organizations also snoop their employees legitimately to monitor their use of organizations' computers and track Internet usage. Answer: C is incorrect. A utility model is an intellectual property right to protect inventions.

QUESTION 46
Which of the following actions does the Data Loss Prevention (DLP) technology take when an agent detects a policy violation for data of all states? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: ABD
Section: Volume A
Explanation

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

QUESTION 47
In which of the following processes are experienced personnel and software tools used to investigate, resolve, and handle process deviation, malformed data, infrastructure, or connectivity issues?

A. Risk Management

B. Exception management
C. Configuration Management
D. Change Management

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Exception management is a process in which experienced personnel and software tools are used to investigate, resolve, and handle process deviation, malformed data, infrastructure or connectivity issues. It increases the efficiency of business processes and contributes in the progress of business. Answer: C is incorrect. Configuration Management (CM) is an Information Technology Infrastructure Library (ITIL) IT Service Management (ITSM) process. It tracks all of the individual Configuration Items (CI) in an IT system, which may be as simple as a single server, or as complex as the entire IT department. In large organizations a configuration manager may be appointed to oversee and manage the CM process. Answer: A is incorrect. Risk Management is used to identify, assess, and control risks. It includes analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats. Risk Management is part of Service Design and the owner of the Risk Management is the Risk Manager. Risks are addressed within several processes in ITIL V3; however, there is no dedicated Risk Management process. ITIL V3 calls for "coordinated risk assessment exercises", so at IT Process Maps we decided to assign clear responsibilities for managing risks. Answer: D is incorrect. Change Management is used to ensure that standardized methods and procedures are used for efficient handling of all changes. A change is "an event that results in a new status of one or more configuration items (CI's)" approved by management, cost effective, enhances business process changes (fixes) - with a minimum risk to IT infrastructure. The main aims of Change Management are as follows: Minimal disruption of services Reduction in back-out activities Economic utilization of resources involved in the change

QUESTION 48
Which of the following rated systems of the Orange book has mandatory protection of the TCB?

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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
Explanation: A B-rated system of the orange book has mandatory protection of the trusted computing base (TCB).
Trusted computing base (TCB) refers to hardware, software, controls, and processes that cause a computer system or network to be devoid of malicious software or hardware. Maintaining the trusted computing base (TCB) is essential for security policy to be implemented successfully.

QUESTION 49
Which of the following is designed to detect unwanted attempts at accessing, manipulating, and disabling of computer systems through the Internet?

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

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

QUESTION 50
Which of the following ensures that a party to a dispute cannot deny the authenticity of their signature on a document or the sending of a message that they originated?

A. Confidentiality
B. OS fingerprinting
C. Reconnaissance
D. Non-repudiation

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:

Explanation: Non-repudiation is a term that refers to the ability to ensure that a party to a dispute cannot deny the authenticity of their signature on a document or the sending of a message that they originated. Non-repudiation is the concept of ensuring that a party in a dispute cannot refuse to acknowledge, or refute the validity of a statement or contract. As a service, it provides proof of the integrity and origin of data. Although this concept can be applied to any transmission, including television and radio, by far the most common application is in the verification and trust of signatures. Answer: A is incorrect. Confidentiality is a mechanism that ensures that only the intended and authorized recipients are able to read data. The data is so encrypted that even if an unauthorized user gets access to it, he will not get any meaning out of it. Answer: C is incorrect. Reconnaissance is a term that refers to information gathering behaviors that aim to profile the organization, employees, network, and systems before an attack is performed efficiently. It is the first step in the process of intrusion and involves unauthorized discovery and mapping of systems, services, or vulnerabilities. These discovery and mapping techniques are commonly known as scanning and enumeration. Common tools, commands, and utilities used for scanning and enumeration include ping, telnet, nslookup, rpcinfo, File Explorer, finger, etc. Reconnaissance activities take place before performing a malicious attack. These activities are used to increase the probability of successful operation against the target, and to increase the probability of hiding the attacker's identity. Answer: B 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.

QUESTION 51

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

Correct Answer: BCD
Section: Volume A
Explanation

Explanation/Reference:

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.

QUESTION 52

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

A. Chosen plaintext attack
B. Chosen ciphertext attack

C. Ciphertext only attack
D. Known plaintext attack

Correct Answer: C
Section: Volume A

Explanation

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

QUESTION 53
The IAM/CA makes certification accreditation recommendations to the DAA. The DAA issues accreditation determinations. Which of the following are the accreditation determinations issued by the DAA? Each correct answer represents a complete solution. Choose all that apply.
A. IATT B.
IATO
C. DATO
D. ATO
E. ATT

Correct Answer: ABCD
Section: Volume A

Explanation

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

QUESTION 54
Which of the following strategies is used to minimize the effects of a disruptive event on a company, and is created to prevent interruptions to normal business activity?

A. Continuity of Operations Plan
B. Contingency Plan

C. Disaster Recovery Plan
D. Business Continuity Plan

Correct Answer: D
Section: Volume B
Explanation

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

QUESTION 55
Which of the following ISO standards provides guidelines for accreditation of an organization that is concerned with certification and registration related to ISMS?

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

Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:
Explanation: ISO 27006 is an information security standard developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is entitled as "Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems". The ISO 27006 standard provides guidelines for accreditation of an organization which is concerned with certification and registration related to ISMS. The ISO 27006 standard contains the following elements: Scope Normative references Terms and definitions Principles General requirements Structural requirements Resource requirements Information requirements Process requirements Management system requirements for certification bodies Information security risk communication Information security risk monitoring and review Annex A. Defining the scope of process Annex B. Asset valuation and impact assessment Annex C. Examples of typical threats Annex D. Vulnerabilities and vulnerability assessment methods Annex E. Information security risk assessment (ISRA) approaches Answer: C is incorrect. The ISO 27003 standard provides guidelines for implementing an ISMS (Information Security Management System). Answer: D is incorrect. The ISO 27004 standard provides guidelines on specifications and use of measurement techniques for the assessment of the effectiveness of an implemented information security management system and controls. Answer: B is incorrect. The ISO 27005 standard provides guidelines for information security risk management.

QUESTION 56
You are advising a school district on disaster recovery plans. In case a disaster affects the main IT centers for the district they will need to be able to work from an alternate location. However, budget is an issue. Which of the following is most appropriate for this client?

A. Cold site
B. Off site
C. Warm site
D. Hot site

Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:
Explanation: A cold site provides an office space, and in some cases basic equipment. However, you will need to restore your data to that equipment in order to use it. This is a much less expensive solution than the hot site. Answer: D is incorrect. A hot site has equipment installed, configured and ready to use. This may make disaster recovery much faster, but will also be more expensive. And a school district can afford to be down for several hours before resuming IT operations, so the less expensive option is more appropriate. Answer: C is incorrect. A warm site is between a hot and cold site. It has some equipment ready and connectivity ready. However, it is still significantly more expensive than a cold site, and not necessary for this scenario. Answer: B is incorrect. Off site is not any type of backup site terminology.

QUESTION 57
Which of the following authentication methods is used to access public areas of a Web site?

A. Anonymous authentication

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

Correct Answer: A
Section: Volume B

Explanation

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

QUESTION 58
Stella works as a system engineer for BlueWell Inc. She wants to identify the performance thresholds of each build. Which of the following tests will help Stella to achieve her task?
A. Reliability test
B. Performance test
C. Regression test
D. Functional test

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
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.

QUESTION 59
Continuous Monitoring is the fourth phase of the security certification and accreditation process. What activities are performed in the Continuous Monitoring process? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: BDE
Section: Volume B
Explanation

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

QUESTION 60
Which of the following terms ensures that no intentional or unintentional unauthorized modification is made to data?
A. Non-repudiation
B. Integrity
C. Authentication
D. Confidentiality

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
Explanation: Integrity ensures that no intentional or unintentional unauthorized modification is made to data. Answer: D is incorrect. Confidentiality refers to the protection of data against unauthorized access. Administrators can provide confidentiality by encrypting data. Answer: A is incorrect. Non-repudiation is a

mechanism to prove that the sender really sent this message. Answer: C is incorrect. Authentication is the process of verifying the identity of a person or network host.

QUESTION 61
Which of the following provides an easy way to programmers for writing lower-risk applications and retrofitting security into an existing application?

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

Correct Answer: B
Section: Volume B
Explanation

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

QUESTION 62
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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
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.

QUESTION 63
Which of the following specifies access privileges to a collection of resources by using the URL mapping?

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

Correct Answer: B
Section: Volume B

Explanation

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

(ITSM) process. It tracks all of the individual Configuration Items (CI) in an IT system, which may be as simple as a single server, or as complex as the entire IT department. In large organizations a configuration manager may be appointed to oversee and manage the CM process.

QUESTION 64
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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
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.

QUESTION 65
Which of the following security models characterizes the rights of each subject with respect to every object in the computer system?

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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation: The access matrix or access control matrix is an abstract, formal security model of protection state in computer systems that characterizes the rights of each subject with respect to every object in the system. It was first introduced by Butler W. Lampson in 1971. According to the access matrix model, the protection state of a computer system can be abstracted as a set of objects 'O', that is the set of entities that needs to be protected (e.g. processes, files, memory

pages) and a set of subjects 'S' that consists of all active entities (e.g. users, processes). Further there exists a set of rights 'R' of the form r(s,o), where s S, o O and r(s,o) R. A right thereby specifies the kind of access a subject is allowed to process with regard to an object. Answer: B is incorrect. The Bell-La Padula Model is a state machine model used for enforcing access control in government and military applications. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g.,"Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public"). The Bell-La Padula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity. Answer: A is incorrect. The ClarkWilson model provides a foundation for specifying and analyzing an integrity policy for a computing system. The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. The model's enforcement and certification rules define data items and processes that provide the basis for an integrity policy. The core of the model is based on the notion of a transaction. Answer: C is incorrect. The Biba model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject.

QUESTION 66
Penetration testing (also called pen testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit. Which of the following areas can be exploited in a penetration test? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: ACDEFG
Section: Volume B
Explanation

Explanation/Reference:
Explanation: Penetration testing (also called pen testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit. Following are the areas that can be exploited in a penetration test: Kernel flaws: Kernel flaws refer to the exploitation of kernel code flaws in the operating system. Buffer overflows: Buffer overflows refer to the exploitation of a software failure to properly check for the length of input data. This overflow can cause malicious behavior on the system. Race conditions: A race condition is a situation in which an attacker can gain access to a system as a privileged user. File and directory permissions: In this area, an attacker exploits weak permissions restrictions to gain unauthorized access of documents. Trojan horses: These are malicious programs that can exploit an information system by attaching themselves in valid programs and files. Social engineering: In this technique, an attacker uses his social skills and persuasion to acquire valuable information that can be used to conduct an attack against a system.

QUESTION 67
Which of the following types of activities can be audited for security? Each correct answer represents a complete solution. Choose three.

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

Correct Answer: ACD
Section: Volume B
Explanation

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

QUESTION 68
Which of the following federal agencies has the objective to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life?

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

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
Explanation: The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. Answer: D is incorrect. The Committee on National Security Systems (CNSS) is a United States intergovernmental organization that sets

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

QUESTION 69
Which of the following SDLC phases consists of the given security controls: Misuse Case Modeling Security Design and Architecture Review Threat and Risk Modeling Security Requirements and Test Cases Generation?

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

Correct Answer: D
Section: Volume B
Explanation

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

QUESTION 70
Which of the following are the initial steps required to perform a risk analysis process? Each correct answer represents a part of the solution. Choose three.

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

Correct Answer: BCD
Section: Volume B
Explanation

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

QUESTION 71
Which of the following technologies is used by hardware manufacturers, publishers, copyright holders and individuals to impose limitations on the usage of digital content and devices?

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

Correct Answer: D

Section: Volume B
Explanation

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

QUESTION 72
Which of the following processes provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and the security posture of a system or site?

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

Correct Answer: B
Section: Volume B

Explanation

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

QUESTION 73
Which of the following security issues does the Bell-La Padula model focus on?

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

Correct Answer: B
Section: Volume B
Explanation

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

QUESTION 74
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

Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:
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: C 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.

QUESTION 75
Which of the following types of obfuscation transformation increases the difficulty for a de-obfuscation tool so that it cannot extract the true application from the obfuscated version?

A. Preventive transformation
B. Data obfuscation
C. Control obfuscation
D. Layout obfuscation

Correct Answer: A
Section: Volume B

Explanation

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

QUESTION 76
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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
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 longdistance 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.

QUESTION 77
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
Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:
Explanation: A distributed denial of service (DDoS) attack targets a Web server with multiple compromised computers that are simultaneously sending hundreds of FIN packets with spoofed IP source IP addresses. DDoS attack occurs when multiple compromised systems flood the bandwidth or resources of a targeted system, usually one or more Web servers. These systems are compromised by attackers using a variety of methods. It is an attempt to make a computer resource unavailable to its intended users. This type of attack can cause the following to occur: Saturate network resources. Disrupt connections between two computers, thereby preventing communications between services. Disrupt services on a specific computer. 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.

QUESTION 78
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++

Correct Answer: AD
Section: Volume B
Explanation

Explanation/Reference:
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.

QUESTION 79
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

Correct Answer: C
Section: Volume B

Explanation

Explanation/Reference:
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.

QUESTION 80
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

Correct Answer: A
Section: Volume B
Explanation
Explanation/Reference:
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.

QUESTION 81
Which of the following refers to a process that is used for implementing information security?

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

Correct Answer: C
Section: Volume B

Explanation

Explanation/Reference:
Explanation: Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The C&A process is used extensively in the U.S. Federal Government. Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. Answer: D is incorrect. Information Assurance (IA) is the practice of managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. While focused dominantly on information in digital form, the full range of IA encompasses not only digital but also analog or physical form. Information assurance as a field has grown from the practice of information security, which in turn grew out of practices and procedures of computer security. Answer: A is incorrect. The classic information security model is used in the practice of Information Assurance (IA) to define assurance requirements. The classic information security model, also called the CIA Triad, addresses three attributes of information and information systems, confidentiality, integrity, and availability. This C-I-A model is extremely useful for teaching introductory and basic concepts of information security and assurance; the initials are an easy mnemonic to remember, and when properly understood, can prompt systems designers and users to address the most pressing aspects of assurance. Answer: B is incorrect. The Five Pillars model is used in the practice of Information Assurance (IA) to define assurance requirements. It was promulgated by the U.S. Department of Defense (DoD) in a variety of publications, beginning with the National Information Assurance Glossary, Committee on National Security Systems Instruction CNSSI-4009. Here is the definition from that publication: "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." The Five Pillars model is sometimes criticized because authentication and non-repudiation are not attributes of information or systems; rather, they are procedures or methods useful to assure the integrity and authenticity of information, and to protect the confidentiality of the same.

QUESTION 82
The Web resource collection is a security constraint element summarized in the Java Servlet Specification v2.4. Which of the following elements does it include? Each correct answer represents a complete solution. Choose two.

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

Correct Answer: AD
Section: Volume B

Explanation

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

QUESTION 83
Which of the following activities are performed by the 'Do' cycle component of PDCA (plan-do-check-act)? Each correct answer represents a complete solution. Choose all that apply.

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

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

QUESTION 84
Numerous information security standards promote good security practices and define frameworks or systems to structure the analysis and design for managing information security controls. Which of the following are the international information security standards? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: BCD
Section: Volume B

Explanation

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

QUESTION 85
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

Correct Answer: AD
Section: Volume B
Explanation

Explanation/Reference:
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: C is incorrect. Simplify the design principle is included in the General Principle 3.

QUESTION 86
SIMULATION
Fill in the blank with the appropriate security mechanism. is a computer hardware mechanism or programming language construct which handles the occurrence of exceptional events.

Correct Answer: Exception handling

Section: Volume B
Explanation

Explanation/Reference:
Explanation: Exception handling is a computer hardware mechanism or programming language construct that handles the occurrence of events. These events occur during the software execution process and interrupt the instruction flow. Exception handling performs the specific activities for managing the exceptional events.

QUESTION 87
In which of the following phases of the DITSCAP process does Security Test and Evaluation (ST&E) occur?

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

Correct Answer: C
Section: Volume B

Explanation

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

QUESTION 88
Which of the following access control models uses a predefined set of access privileges for an object of a system?

A. Role-Based Access Control
B. Discretionary Access Control

C. Policy Access Control
D. Mandatory Access Control

Correct Answer: D
Section: Volume B
Explanation

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

QUESTION 89
Martha works as a Project Leader for BlueWell Inc. She and her team have developed accounting software. The software was performing well. Recently, the software has been modified. The users of this software are now complaining about the software not working properly. Which of the following actions will she take to test the software?

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

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
Explanation: Regression testing can be performed any time when a program needs to be modified either to add a feature or to fix an error. It is a process of repeating Unit testing and Integration testing whenever existing tests need to be performed again along with the new tests. Regression testing is performed to ensure that no existing errors reappear, and no new errors are introduced. Answer: D is incorrect. The acceptance testing is performed on the application before its implementation into the production environment. It is done either by a client or an application specialist to ensure that the software meets the requirement for which it was made. Answer: A is incorrect. Integration testing is a logical extension of unit testing. It is performed to identify the problems that occur when two or more

units are combined into a component. During integration testing, a developer combines two units that have already been tested into a component, and tests the interface between the two units. Although integration testing can be performed in various ways, the following three approaches are generally used: The top-down approach The bottom-up approach The umbrella approach Answer: C 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.

QUESTION 90
Which of the following sections come under the ISO/IEC 27002 standard?

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

Correct Answer: ABD
Section: Volume B
Explanation

Explanation/Reference:
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: C is incorrect. Financial assessment does not come under the ISO/IEC 27002 standard.

QUESTION 91
Which of the following statements about the authentication concept of information security management is true?

A. It establishes the users' identity and ensures that the users are who they say they are.
B. It ensures the reliable and timely access to resources.
C. It determines the actions and behaviors of a single individual within a system, and identifies that particular individual.

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

Correct Answer: A
Section: Volume B
Explanation

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

QUESTION 92
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.

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
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: C 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.

QUESTION 93
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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
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.

QUESTION 94
In which of the following DIACAP phases is residual risk analyzed?

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

Correct Answer: D
Section: Volume B

Explanation

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

QUESTION 95
Which of the following security controls will you use for the deployment phase of the SDLC to build secure software? Each correct answer represents a complete solution. Choose all that apply.

A. Change and Configuration Control

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

Correct Answer: BCD
Section: Volume B
Explanation

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

QUESTION 96
Which of the following provides an easy way to programmers for writing lower-risk applications and retrofitting security into an existing application?

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

Correct Answer: D
Section: Volume B
Explanation

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

QUESTION 97
Which of the following methods can be helpful to eliminate social engineering threat? Each correct answer represents a complete solution. Choose three.

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

Correct Answer: ABD
Section: Volume B
Explanation

Explanation/Reference:
Explanation: The following methods can be helpful to eliminate social engineering threat: Password policies Vulnerability assessments Data classification Password policy should specify that how the password can be shared. Company should implement periodic penetration and vulnerability assessments. These assessments usually consist of using known hacker tools and common hacker techniques to breach a network security. Social engineering should also be used for an accurate assessment. Since social engineers use the knowledge of others to attain information, it is essential to have a data classification model in place that all employees know and follow. Data classification assigns level of sensitivity of company information. Each classification level specifies that who can view and edit data, and how it can be shared.

QUESTION 98
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.

Correct Answer: ABD
Section: Volume B
Explanation

Explanation/Reference:
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.

QUESTION 99
Which of the following types of attacks occurs when an attacker successfully inserts an intermediary software or program between two communicating hosts?

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

Correct Answer: C
Section: Volume B

Explanation

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

QUESTION 100
Which of the following is an example of penetration testing?

A. Implementing NIDS on a network
B. Implementing HIDS on a computer
C. Simulating an actual attack on a network
D. Configuring firewall to block unauthorized traffic

Correct Answer: C
Section: Volume B

Explanation

Explanation/Reference:
Explanation: Penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source, known as a Black Hat Hacker, or Cracker. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the

system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The intent of a penetration testing is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered. It is a component of a full security audit. Answer: A, B, and D are incorrect. Implementing NIDS and HIDS and configuring firewall to block unauthorized traffic are not examples of penetration testing.

QUESTION 101
Which of the following security controls works as the totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy?

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

Correct Answer: C
Section: Volume B

Explanation

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

QUESTION 102
You are responsible for network and information security at a large hospital. It is a significant concern that any change to any patient record can be easily traced back to the person who made that change. What is this called?

A. Availability
B. Confidentiality
C. Non repudiation

D. Data Protection

Correct Answer: C
Section: Volume B

Explanation

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

QUESTION 103
In which of the following deployment models of cloud is the cloud infrastructure operated exclusively for an organization?

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

Correct Answer: C
Section: Volume B

Explanation

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

QUESTION 104
The Software Configuration Management (SCM) process defines the need to trace changes, and the ability to verify that the final delivered software has all of the planned enhancements that are supposed to be included in the release. What are the procedures that must be defined for each software project to ensure that a sound SCM process is implemented? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: ABCD
Section: Volume B
Explanation

Explanation/Reference:
Explanation: The SCM process defines the need to trace changes, and the ability to verify that the final delivered software has all of the planned enhancements that are supposed to be included in the release. It identifies four procedures that must be defined for each software project to ensure that a sound SCM process is implemented. They are as follows: 1.Configuration identification: Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined. 2.Configuration change control: Configuration change control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them. 3.Configuration status accounting: Configuration status accounting is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time. 4.Configuration audits: Configuration audits are broken into functional and physical configuration audits. They occur either at delivery or at the moment of effecting the change. A functional configuration audit ensures that functional and performance attributes of a configuration item are achieved, while a physical configuration audit ensures that a configuration item is installed in accordance with the requirements of its detailed design documentation.

QUESTION 105
At which of the following levels of robustness in DRM must the security functions be immune to widely available tools and specialized tools and resistant to professional tools?

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

Correct Answer: C
Section: Volume B

Explanation

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

QUESTION 106
Which of the following plans is designed to protect critical business processes from natural or man-made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes?

A. Contingency plan
B. Business continuity plan
C. Crisis communication plan
D. Disaster recovery plan

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
Explanation: The business continuity plan is designed to protect critical business processes from natural or man-made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan. Answer: C is incorrect. The crisis communication plan can be broadly defined as the plan for the exchange of information before, during, or after a crisis event. It is considered as a sub-specialty of the public relations profession that is designed to protect and defend an individual, company, or organization facing a public challenge to its reputation. The aim of crisis communication plan is to assist organizations to achieve continuity of critical business processes and information flows under crisis, disaster or event driven circumstances. Answer: A is incorrect. A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and "triggers" for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption. Answer: D is incorrect. A disaster recovery plan should contain data, hardware, and software that can be critical for a business. It should also include the plan for sudden loss such as hard disc crash. The business should use backup and data recovery utilities to limit the loss of data.

QUESTION 107

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

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

Correct Answer: D
Section: Volume B
Explanation

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

QUESTION 108
Which of the following tiers addresses risks from an information system perspective?

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

Correct Answer: B
Section: Volume B

Explanation

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

description. Answer: D is incorrect. The Organization Level is the Tier 1, and it addresses risks from an organizational perspective. Answer: C is incorrect. The mission and business process level is the Tier 2, and it addresses risks from the mission and business process perspective.

QUESTION 109
Mark works as a Network Administrator for NetTech Inc. The company has a Windows 2000 domain-based network. Users report that they are unable to log on to the network. Mark finds that accounts are locked out due to multiple incorrect log on attempts. What is the most likely cause of the account lockouts?

A. Spoofing
B. Brute force attack
C. SYN attack
D. PING attack

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
Explanation: Brute force attack is the most likely cause of the account lockouts. In a brute force attack, unauthorized users attempt to log on to a network or a computer by using multiple possible user names and passwords. Windows 2000 and other network operating systems have a security feature that locks a user account if the number of failed logon attempts occur within a specified period of time, based on the security policy lockout settings. Answer: A is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting online, etc. because forging the source IP address causes the responses to be misdirected. Answer: C is incorrect. A SYN attack affects computers running on the TCP/IP protocol. It is a protocol-level attack that can render a computer's network services unavailable. A SYN attack is also known as SYN flooding. Answer: D is incorrect. When a computer repeatedly sends ICMP echo requests to another computer, it is known as a PING attack.

QUESTION 110
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

Correct Answer: BCDE

Section: Volume B
Explanation

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

QUESTION 111
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

Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:
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.

QUESTION 112
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

Correct Answer: C
Section: Volume B

Explanation

Explanation/Reference:
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.

QUESTION 113
The Project Risk Management knowledge area focuses on which of the following processes? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: ABC
Section: Volume B
Explanation

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

QUESTION 114
Which of the following is used by attackers to record everything a person types, including usernames, passwords, and account information?

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

Correct Answer: B
Section: Volume B

Explanation

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

QUESTION 115
Which of the following policies can explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations?

A. Informative
B. Advisory
C. Selective
D. Regulatory

Correct Answer: A
Section: Volume B

Explanation

Explanation/Reference:
Explanation: An informative policy informs employees about certain topics. It is not an enforceable policy, but rather one to teach individuals about specific issues relevant to the company. The informative policy can explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations. Answer: D is incorrect. A regulatory policy ensures that an organization follows the standards set by specific industry regulations. This type of policy is very detailed and specific to a type of industry. The regulatory policy is used in financial institutions, health care facilities, public utilities, and other government-regulated industries, e.g., TRAI. Answer: B is incorrect. An advisory policy strongly advises employees regarding which types of behaviors and activities should and should not take place within the organization. It also outlines possible ramifications if employees do not comply with the established behaviors

and activities. The advisory policy can be used to describe how to handle medical information, handle financial transactions, and process confidential information.
Answer: C is incorrect. It is not a valid type of policy.

QUESTION 116
Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?

A. Single Loss Expectancy (SLE)
B. Annualized Rate of Occurrence (ARO)
C. Safeguard
D. Exposure Factor (EF)

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
Explanation: The Annualized Rate of Occurrence (ARO) is a number that represents the estimated frequency at 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. Answer: D is incorrect. The Exposure Factor (EF) represents the % of assets loss caused by a threat. The EF is required to calculate the Single Loss Expectancy (SLE). Answer: A is incorrect. The Single Loss Expectancy (SLE) is the value in dollars that is assigned to a single event. SLE = Asset Value ($) X Exposure Factor (EF) Answer: C is incorrect. Safeguard acts as a countermeasure for reducing the risk associated with a specific threat or a group of threats.

QUESTION 117
What are the subordinate tasks of the Implement and Validate Assigned IA Control phase in the DIACAP process? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: ABC
Section: Volume B
Explanation

Explanation/Reference:

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

QUESTION 118
Which of the following is an open source network intrusion detection system?

A. NETSH
B. Macof
C. Sourcefire
D. Snort

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation: Snort is an open source network intrusion prevention and detection system that operates as a network sniffer. It logs activities of the network that is matched with the predefined signatures. Signatures can be designed for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP). The three main modes in which Snort can be configured are as follows:

Sniffer mode: It reads the packets of the network and displays them in a continuous stream on the console. Packet logger mode: It logs the packets to the disk. Network intrusion detection mode: It is the most complex and configurable configuration, allowing Snort to analyze network traffic for matches against a userdefined rule set. Answer: B is incorrect. Macof is a tool of the dsniff tool set and used to flood the local network with random MAC addresses. It causes some switches to fail open in repeating mode, and facilitates sniffing. Answer: C is incorrect. Sourcefire is the company that owns and maintains Snort. Answer: A is incorrect. NETSH is not a network intrusion detection system. NETSH is a command line tool to configure TCP/IP settings such as the IP address, Subnet Mask, Default Gateway, DNS, WINS addresses, etc.

QUESTION 119
You work as a Security Manager for Tech Perfect Inc. The company has a Windows based network. It is required to determine compatibility of the systems with custom applications. Which of the following techniques will you use to accomplish the task?

A. Safe software storage
B. Antivirus management
C. Backup control
D. Software testing

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation: In order to accomplish the task, you should use the software testing technique. By using this technique you can determine compatibility of systems with custom applications or you can identify other unforeseen interactions. You can also use the software testing technique while you are upgrading software. Answer: B is incorrect. You can use the antivirus management to save the systems from viruses, unexpected software interactions, and the subversion of security controls. Answer: A is incorrect. You can use the safe software storage technique to ensure that the software and backup copies have not been modified without authorization. Answer: C is incorrect. You can use the backup control to perform back up of software and data.

QUESTION 120
Adrian is the project manager of the NHP Project. In her project there are several work packages that deal with electrical wiring. Rather than to manage the risk internally she has decided to hire a vendor to complete all work packages that deal with the electrical wiring. By removing the risk internally to a licensed electrician Adrian feels more comfortable with project team being safe. What type of risk response has Adrian used in this example?

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

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation: This is an example of transference. When the risk is transferred to a third party, usually for a fee, it creates a contractual-relationship for the third party to manage the risk on behalf of the performing organization. Risk response planning is a method of developing options to decrease the amount of threats and make the most of opportunities. The risk response should be aligned with the consequence of the risk and cost-effectiveness. This planning documents the processes for managing risk events. It addresses the owners and their responsibilities, risk identification, results from qualification and quantification processes, budgets and times for responses, and contingency plans. The various risk response planning techniques are as follows: Risk acceptance: It indicates that the project team has decided not to change the project management plan to deal with a risk, or is unable to identify any other suitable response strategy. Risk avoidance: It is a technique for a threat, which creates changes to the project management plan that are meant to either eliminate the risk or to protect the project objectives from this impact. Risk mitigation: It is a list of specific actions being taken to deal with specific risks associated with the threats and seeks to reduce the probability of occurrence or impact of risk below an acceptable threshold. Risk transference: It is used to shift the impact of a threat to a third party, together with the ownership of the response.

QUESTION 121

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

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

Correct Answer: D
Section: Volume C

Explanation

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

QUESTION 122
Which of the following is the most secure method of authentication?

A. Biometrics
B. Username and password
C. Anonymous
D. Smart card

Correct Answer: A
Section: Volume C

Explanation

Explanation/Reference:
Explanation: Biometrics is a method of authentication that uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user. Nowadays, the usage of biometric devices such as hand scanners and retinal scanners is becoming more common in the business environment. It is the most secure method of authentication. Answer: B is incorrect. Username and password is the least secure method of authentication in comparison of smart card and biometrics authentication. Username and password can be intercepted. Answer: D is incorrect. Smart card authentication is not as reliable as biometrics authentication. Answer: C is incorrect. Anonymous authentication does not provide security as a user can log on to the system anonymously and he is not prompted for credentials.

QUESTION 123
Maria has been recently appointed as a Network Administrator in Gentech Inc. She has been tasked to perform network security testing to find out the vulnerabilities and shortcomings of the present network infrastructure. Which of the following testing approaches will she apply to accomplish this task?

A. Gray-box testing
B. White-box testing
C. Black-box testing
D. Unit testing

Correct Answer: C
Section: Volume C

Explanation

Explanation/Reference:
Explanation: Maria is new for this organization and she does not have any idea regarding the present infrastructure. Therefore, black box testing is best suited for her. Blackbox testing is a technique in which the testing team has no knowledge about the infrastructure of the organization. The testers must first determine the location and extent of the systems before commencing their analysis. This testing technique is costly and time consuming. Answer: B is incorrect. White box testing, also known as Clear box or Glass box testing, takes into account the internal mechanism of a system or application. The connotations of "Clear box" and "Glass box" indicate that a tester has full visibility of the internal workings of the system. It uses knowledge of the internal structure of an application. It is applicable at the unit, integration, and system levels of the software testing process. It consists of the following testing methods: Control flow-based testing Create a graph from source code. Describe the flow of control through the control flow graph. Design test cases to cover certain elements of the graph. Data flow-based testing Test connections between variable definitions. Check variation of the control flow graph. Set DEF (n) contains variables that are defined at node n. Set USE (n) are variables that are read. Answer: A is incorrect. 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: D 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.

QUESTION 124

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

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

Correct Answer: C
Section: Volume C
Explanation

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

QUESTION 125
The Phase 3 of DITSCAP C&A is known as Validation. The goal of Phase 3 is to validate that the preceding work has produced an IS that operates in a specified computing environment. What are the process activities of this phase? Each correct answer represents a complete solution. Choose all that apply.

A. Certification and accreditation decision
B. Continue to review and refine the SSAA
C. Perform certification evaluation of the integrated system
D. System development
E. Develop recommendation to the DAA

Correct Answer: ABCE
Section: Volume C
Explanation

Explanation/Reference:
Explanation: The Phase 3 of DITSCAP C&A is known as Validation. The goal of Phase 3 is to validate that the preceding work has produced an IS that operates in a specified computing environment. The process activities of this phase are as follows: Continue to review and refine the SSAA Perform certification evaluation of the integrated system Develop recommendation to the DAA Certification and accreditation decision Answer: D is incorrect. System development is a Phase 2 activity.

QUESTION 126
Which of the following methods 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?

A. Configuration control
B. Documentation control
C. Configuration identification
D. Configuration auditing

Correct Answer: B
Section: Volume C

Explanation

Explanation/Reference:
Explanation: Documentation control is a method of ensuring that system changes should be agreed upon before being implemented, only the proposed and approved changes are implemented, and the implementation is complete and accurate. Documentation control is involved in the strict events for proposing, monitoring, and approving system changes and their implementation. It helps the change process by supporting the person who synchronizes the analytical task, approves system changes, reviews the implementation of changes, and oversees other tasks such as documenting the controls. Answer: D 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. 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: C 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.

QUESTION 127

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

Correct Answer: ABD
Section: Volume C
Explanation

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

QUESTION 128
What NIACAP certification levels are recommended by the certifier? Each correct answer represents a complete solution. Choose all that apply.

A. Comprehensive Analysis
B. Maximum Analysis
C. Detailed Analysis
D. Minimum Analysis
E. Basic Security Review
F. Basic System Review

Correct Answer: ACDE
Section: Volume C
Explanation

Explanation/Reference:
Explanation: NIACAP has four levels of certification. These levels ensure that the appropriate C&A are performed for varying schedule and budget limitations. The certifier must analyze the system's business functions. The certifier determines the degree of confidentiality, integrity, availability, and accountability, and then

recommends one of the following NIACAP certification levels: Level 1 - Basic Security Review Level 2 - Minimum Analysis Level 3 - Detailed Analysis Level 4 Comprehensive Analysis Answer: B and F are incorrect. No such types of levels exist.

QUESTION 129
Which of the following intrusion detection systems (IDS) monitors network traffic and compares it against an established baseline?

A. File-based
B. Network-based
C. Anomaly-based
D. Signature-based

Correct Answer: C
Section: Volume C

Explanation

Explanation/Reference:
Explanation: The anomaly-based intrusion detection system (IDS) monitors network traffic and compares it against an established baseline. This type of IDS monitors traffic and system activity for unusual behavior based on statistics. In order to identify a malicious activity, it learns normal behavior from the baseline. The anomaly-based intrusion detection is also known as behavior-based or statistical-based intrusion detection. Answer: D is incorrect. Signature-based IDS uses a database with signatures to identify possible attacks and malicious activity. Answer: B is incorrect. A network-based IDS can be a dedicated hardware appliance, or an application running on a computer, attached to the network. It monitors all traffic in a network or traffic coming through an entry-point such as an Internet connection. Answer: A is incorrect. There is no such intrusion detection system (IDS) that is file-based.

QUESTION 130
Which of the following characteristics are described by the DIAP Information Readiness Assessment function? Each correct answer represents a complete solution. Choose all that apply.

A. It provides for entry and storage of individual system data.
B. It performs vulnerability/threat analysis assessment.
C. It provides data needed to accurately assess IA readiness.
D. It identifies and generates IA requirements.

Correct Answer: BCD
Section: Volume C
Explanation

Explanation/Reference:

Explanation: The characteristics of the DIAP Information Readiness Assessment function are as follows: It provides data needed to accurately assess IA readiness. It identifies and generates IA requirements. It performs vulnerability/threat analysis assessment. Answer: A is incorrect. It is a function performed by the ASSET system.

QUESTION 131
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

Correct Answer: D
Section: Volume C

Explanation

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

QUESTION 132
Which of the following security design principles supports comprehensive and simple design and implementation of protection mechanisms, so that an unintended access path does not exist or can be readily identified and eliminated?

.

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

Correct Answer: B
Section: Volume C

Explanation

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

QUESTION 133
Rob is the project manager of the IDLK Project for his company. This project has a budget of $5,600,000 and is expected to last 18 months. Rob has learned that a new law may affect how the project is allowed to proceed - even though the organization has already invested over $750,000 in the project. What risk response is the most appropriate for this instance?

A. Transference
B. Enhance
C. Mitigation
D. Acceptance

Correct Answer: D
Section: Volume C

Explanation

Explanation/Reference:
Explanation: At this point all that Rob can likely do is accepting the risk event. Because this is an external risk, there is little that Rob can do other than document the risk and share the new with management and the project stakeholders. If the law is passed then Rob can choose the most appropriate way for the project to continue. Acceptance response is a part of Risk Response planning process. Acceptance response delineates that the project plan will not be changed to deal with

the risk. Management may develop a contingency plan if the risk does occur. Acceptance response to a risk event is a strategy that can be used for risks that pose either threats or opportunities. Acceptance response can be of two types: Passive acceptance: It is a strategy in which no plans are made to try or avoid or mitigate the risk. Active acceptance: Such responses include developing contingency reserves to deal with risks, in case they occur. Acceptance is the only response for both threats and opportunities. Answer: B is incorrect. Mitigation aims to lower the probability and/or impact of the risk event. Answer: C is incorrect. Transference transfers the ownership of the risk event to a third party, usually through a contractual agreement. Answer: D is incorrect. Enhance is a risk response that tries to increase the probability and/or impact of the positive risk event.

QUESTION 134
Mark is the project manager of the NHQ project in StarTech Inc. The project has an asset valued at $195,000 and is subjected to an exposure factor of 35 percent. What will be the Single Loss Expectancy of the project?

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

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:
Explanation: The Single Loss Expectancy (SLE) of this project will be $68,250. Single Loss Expectancy is a term related to Risk Management and Risk Assessment. It can be defined as the monetary value expected from the occurrence of a risk on an asset. It is mathematically expressed as follows: Single Loss Expectancy (SLE) = Asset Value (AV) * Exposure Factor (EF) where the Exposure Factor is represented in the impact of the risk over the asset, or percentage of asset lost. As an example, if the Asset Value is reduced two thirds, the exposure factor value is .66. If the asset is completely lost, the Exposure Factor is 1.0. The result is a monetary value in the same unit as the Single Loss Expectancy is expressed. Here, it is as follows: SLE = Asset Value * Exposure Factor
= 195,000 * 0.35
= $68,250
Answer: B, C, and D are incorrect. These are not valid SLE's for this project.

QUESTION 135
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.

Correct Answer: ABCD
Section: Volume C
Explanation

Explanation/Reference:
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.

QUESTION 136
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He finds that the We-are-secure server is vulnerable to attacks. As a countermeasure, he suggests that the Network Administrator should remove the IPP printing capability from the server. He is suggesting this as a countermeasure against _____.

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

Correct Answer: B
Section: Volume C

Explanation

Explanation/Reference:
Explanation: Removing the IPP printing capability from a server is a good countermeasure against an IIS buffer overflow attack. A Network Administrator should take the following steps to prevent a Web server from IIS buffer overflow attacks: Conduct frequent scans for server vulnerabilities. Install the upgrades of Microsoft service packs.
Implement effective firewalls. Apply URLScan and IISLockdown utilities. Remove the IPP printing capability. Answer: D is incorrect. The following are the DNS zone transfer countermeasures: Do not allow DNS zone transfer using the DNS property sheet: a.Open DNS. b.Right-click a DNS zone and click Properties. c.On the Zone Transfer tab, clear the Allow zone transfers check box. Configure the master DNS server to allow zone transfers only from secondary DNS servers: a.Open DNS. b.Right-click a DNS zone and click Properties. c.On the zone transfer tab, select the Allow zone transfers check box, and then do one of the following: To allow zone transfers only to the DNS servers listed on the name servers tab, click on the Only to the servers listed on the Name Server tab. To allow zone transfers only to specific DNS servers, click Only to the following servers, and add the IP address of one or more servers. Deny all unauthorized inbound connections to TCP port 53. Implement DNS keys and encrypted DNS payloads. Answer: A is incorrect. The following are the countermeasures against SNMP enumeration:
1.Removing the SNMP agent or disabling the SNMP service 2.Changing the default PUBLIC community name when 'shutting off SNMP' is not an option

3.Implementing the Group Policy security option called Additional restrictions for anonymous connections 4.Restricting access to NULL session pipes and NULL session shares 5.Upgrading SNMP Version 1 with the latest version 6.Implementing Access control list filtering to allow only access to the read-write community from approved stations or subnets Answer: C is incorrect. NetBIOS NULL session vulnerabilities are hard to prevent, especially if NetBIOS is needed as part of the infrastructure. One or more of the following steps can be taken to limit NetBIOS NULL session vulnerabilities: 1.Null sessions require access to the TCP 139 or TCP 445 port, which can be disabled by a Network Administrator. 2.A Network Administrator can also disable SMB services entirely on individual hosts by unbinding
WINS Client TCP/IP from the interface. 3.A Network Administrator can also restrict the anonymous user by editing the registry values: a.Open regedit32, and go to HKLM\SYSTEM\CurrentControlSet\LSA. b.Choose edit > add value. Value name: RestrictAnonymous Data Type: REG_WORD Value: 2

QUESTION 137
Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in. What are the different categories of penetration testing? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: ABCEF
Section: Volume C
Explanation

Explanation/Reference:
Explanation: The different categories of penetration testing are as follows: Open-box: In this category of penetration testing, testers have access to internal system code. This mode is basically suited for Unix or Linux. Closed-box: In this category of penetration testing, testers do not have access to closed systems. This method is good for closed systems. Zero-knowledge test: In this category of penetration testing, testers have to acquire information from scratch and they are not supplied with information concerning the IT system. Partial-knowledge test: In this category of penetration testing, testers have knowledge that may be applicable to a specific type of attack and associated vulnerabilities. Full-knowledge test: In this category of penetration testing, testers have massive knowledge concerning the information system to be evaluated. Answer: D is incorrect. There is no such category of penetration testing.

QUESTION 138
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

Correct Answer: C
Section: Volume C

Explanation

Explanation/Reference:
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.

QUESTION 139
Which of the following statements reflect the 'Code of Ethics Canons' in the '(ISC)2 Code of Ethics'? Each correct answer represents a complete solution. Choose all that apply.

A. Act honorably, honestly, justly, responsibly, and legally.
B. Give guidance for resolving good versus good and bad versus bad dilemmas.
C. Provide diligent and competent service to principals.
D. Protect society, the commonwealth, and the infrastructure.

Correct Answer: ACD
Section: Volume C
Explanation

Explanation/Reference:
Explanation: The Code of Ethics Canons in (ISC)2 code of ethics are as follows: Protect society, the commonwealth, and the infrastructure. Act honorably, honestly, justly, responsibly, and legally. Provide diligent and competent service to principals. Advance and protect the profession.

QUESTION 140

The Systems Development Life Cycle (SDLC) is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems. Which of the following are the different phases of system development life cycle? Each correct answer represents a complete solution. Choose all that apply.

A. Testing B.
Implementation
C. Operation/maintenance
D. Development/acquisition
E. Disposal
F. Initiation

Correct Answer: BCDEF
Section: Volume C
Explanation

Explanation/Reference:
Explanation: The Systems Development Life Cycle (SDLC), or Software Development Life Cycle in systems engineering, information systems, and software engineering, is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems. The concept generally refers to computers or information systems. The following are the five phases in a generic System Development Life Cycle: 1.Initiation
2.Development/acquisition
3.Implementation 4.Operation/maintenance 5.Disposal

QUESTION 141
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

Correct Answer: C
Section: Volume C

Explanation

Explanation/Reference:

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.

QUESTION 142
Which of the following concepts represent the three fundamental principles of information security? Each correct answer represents a complete solution. Choose three.

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

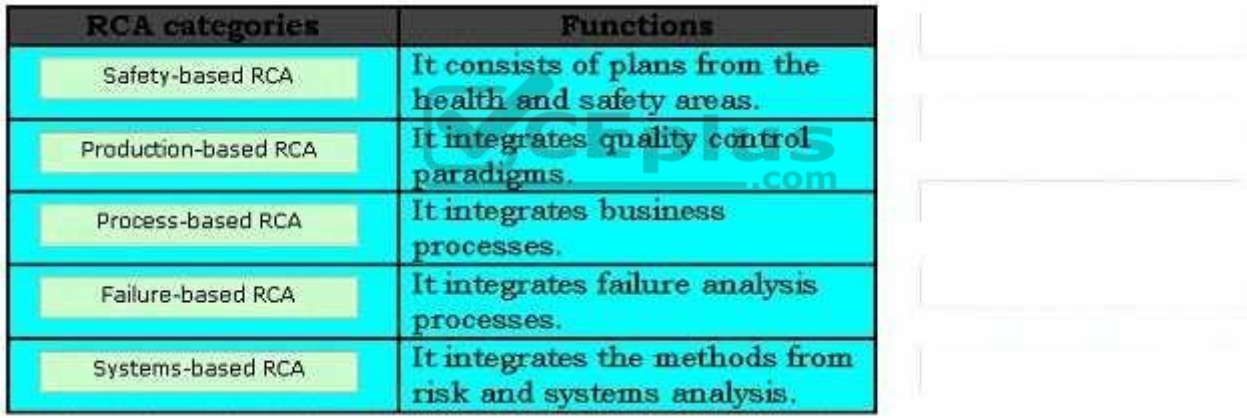
Correct Answer: BCD
Section: Volume C
Explanation

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

QUESTION 143
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.

Select and Place:

Correct Answer:



Section: Volume C
Explanation

Explanation/Reference:
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.

QUESTION 144

Samantha works as an Ethical Hacker for we-are-secure Inc. She wants to test the security of the we-are-secure server for DoS attacks. She sends large number of ICMP ECHO packets to the target computer. Which of the following DoS attacking techniques will she use to accomplish the task?

A. Smurf dos attack
B. Land attack
C. Ping flood attack
D. Teardrop attack

Correct Answer: C
Section: Volume C

Explanation

Explanation/Reference:
Explanation: According to the scenario, Samantha is using the ping flood attack. In a ping flood attack, an attacker sends a large number of ICMP packets to the target computer using the ping command, i.e., ping -f target_IP_address. When the target computer receives these packets in large quantities, it does not respond and hangs. However, for such an attack to take place, the attacker must have sufficient Internet bandwidth, because if the target responds with an "ECHO reply ICMP packet" message, the attacker must have both the incoming and outgoing bandwidths available for communication. Answer: A is incorrect. In a smurf DoS attack, an attacker sends a large amount of ICMP echo request traffic to the IP broadcast addresses. These ICMP requests have a spoofed source address of the intended victim. If the routing device delivering traffic to those broadcast addresses delivers the IP broadcast to all the hosts, most of the IP addresses send an ECHO reply message. However, on a multi- access broadcast network, hundreds of computers might reply to each packet when the target network is overwhelmed by all the messages sent simultaneously. Due to this, the network becomes unable to provide services to all the messages and crashes. Answer: D is incorrect. In a teardrop attack, a series of data packets are sent to the target computer with overlapping offset field values. As a result, the target computer is unable to reassemble these packets and is forced to crash, hang, or reboot. Answer: B is incorrect. In a land attack, the attacker sends a spoofed TCP SYN packet in which the IP address of the target is filled in both the source and destination fields. On receiving the spoofed packet, the target system becomes confused and goes into a frozen state. Now-a-days, antivirus can easily detect such an attack.

QUESTION 145
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

Correct Answer: BCD
Section: Volume C
Explanation

Explanation/Reference:
Explanation: The following procedural patterns are defined by the DARPA paper in order to perform secure software development practices: Build the server from the ground up: It includes the following features: Build the server from the ground up. Identify the default installation of the operating system and applications. Support hardening procedures to remove unnecessary services. Identify a vulnerable service for ongoing risk management. Choose the right stuff: It defines guidelines to select right commercial off-the-shelf (COTS) components and decide whether to use and build custom components. Document the server configuration: It supports the creation of an initial configuration baseline and tracks all modifications made to servers and application configurations.
Patch proactively: It supports in applying patches as soon as they are available rather than waiting until the systems cooperate. Red team the design: It supports an independent security assessment from the perspective of an attacker in the quality assurance or testing stage. An independent security assessment is helpful in addressing a security issue before it occurs. 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.

QUESTION 146
In which of the following SDLC phases is the system's security features configured and enabled, the system is tested and installed or fielded, and the system is authorized for processing?

A. Development/Acquisition Phase
B. Operation/Maintenance Phase
C. Implementation Phase
D. Initiation Phase

Correct Answer: C
Section: Volume C

Explanation

Explanation/Reference:
Explanation: It is the implementation phase, in which the system's security features are configured and enabled, the system is tested and installed or fielded, and the system is authorized for processing. A design review and systems test should be performed prior to placing the system into operation to ensure that it meets security specifications. Answer: B is incorrect. In Operation/Maintenance Phase, the system performs its work. The system is almost always being continuously modified by the addition of hardware and software and by numerous other events. Answer: D is incorrect. In the initiation phase, the need for a system is expressed and the purpose of the system is documented. Answer: A is incorrect. In Development/Acquisition Phase, the system is designed, purchased, programmed, developed, or otherwise constructed.

QUESTION 147
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

Correct Answer: D
Section: Volume C

Explanation

Explanation/Reference:
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.

QUESTION 148
Which of the following test methods has the objective to test the IT system from the viewpoint of a threat-source and to identify potential failures in the IT system protection schemes?

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

Correct Answer: B
Section: Volume C

Explanation

Explanation/Reference:

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

QUESTION 149
Which of the following documents is defined as a source document, which is most useful for the ISSE when classifying the needed security functionality?

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

Correct Answer: A
Section: Volume C

Explanation

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

QUESTION 150
You work as the Senior Project manager in Dotcoiss Inc. Your company has started a software project using configuration management and has completed 70% of it. You need to ensure that the network infrastructure devices and networking standards used in this project are installed in accordance with the requirements of its detailed project design documentation. Which of the following procedures will you employ to accomplish the task?

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

Correct Answer: D
Section: Volume C

Explanation

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

QUESTION 151
FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls are tested and reviewed?

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

Correct Answer: A
Section: Volume C
Explanation
Explanation/Reference:
Explanation: The following are the five levels of FITSAF based on SEI's Capability Maturity Model (CMM): Level 1: The first level reflects that an asset has documented a security policy. Level 2: The second level shows that the asset has documented procedures and controls to implement the policy. Level 3: The third level indicates that these procedures and controls have been implemented. Level 4: The fourth level shows that the procedures and controls are tested and reviewed. Level 5: The fifth level is the final level and shows that the asset has procedures and controls fully integrated into a comprehensive program.

QUESTION 152
Which of the following ISO standards is entitled as "Information technology - Security techniques - Information security management - Measurement"?

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

Correct Answer: C
Section: Volume C

Explanation

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

QUESTION 153
Which of the following processes will you involve to perform the active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures?

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

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

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

QUESTION 154
Which of the following are the responsibilities of the owner with regard to data in an information classification program? Each correct answer represents a complete solution. Choose three.

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

Correct Answer: ACD
Section: Volume C
Explanation

Explanation/Reference:
Explanation: The following are the responsibilities of the owner with regard to data in an information classification program: Determining what level of classification the information requires. Reviewing the classification assignments at regular time intervals and making changes as the business needs change. Delegating the responsibility of the data protection duties to a custodian. An information owner can be an executive or a manager of an organization. He will be responsible for the asset of information that must be protected. Answer: B is incorrect. Running regular backups and routinely testing the validity of the backup data is the responsibility of a custodian.

QUESTION 155
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

Correct Answer: D
Section: Volume C

Explanation

Explanation/Reference:
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: C is incorrect. Mitigation is a risk response planning technique associated with threats that seeks to reduce the probability of occurrence or impact of a risk to below an acceptable threshold. Risk mitigation involves taking early action to reduce the probability and impact of a risk occurring on the project. Adopting less complex processes, conducting more tests, or choosing a more stable supplier are examples of mitigation actions. Answer: A is incorrect. Avoidance involves changing the project management plan to eliminate the threat entirely. Answer: B is incorrect. Acceptance response is a part of Risk Response planning process. Acceptance response delineates that the project plan will not be changed to deal with the risk. Management may develop a contingency plan if the risk does occur. Acceptance response to a risk event is a strategy that can be used for risks that pose either threats or opportunities. Acceptance response can be of two types: Passive acceptance: It is a strategy in which no plans are made to try or avoid or mitigate the risk. Active acceptance: Such responses include developing contingency reserves to deal with risks, in case they occur. Acceptance is the only response for both threats and opportunities.

QUESTION 156
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

Correct Answer: A
Section: Volume C

Explanation

Explanation/Reference:
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-

instages, in an effort to combine advantages of top-down and bottom-up concepts. The basic principles of the spiral model are as follows: The focus is on risk assessment and minimizing project risks by breaking a project into smaller segments and providing more ease-of- change during the development process, as well as providing the opportunity to evaluate risks and weigh consideration of project continuation throughout the life cycle. Each cycle involves a progression through the same sequence of steps, for each portion of the product and for each of its levels of elaboration, from an overall concept-of-operation document down to the coding of each individual program. Each trip around the spiral traverses the following four basic quadrants: Determine objectives, alternatives, and constraints of the iteration. Evaluate alternatives, and identify and resolve risks. Develop and verify deliverables from the iteration. Plan the next iteration.
Begin each cycle with an identification of stakeholders and their win conditions, and end each cycle with review and commitment. Answer: D is incorrect. The Prototyping model is a systems development method (SDM). In this model, a prototype is created, tested, and then reworked as necessary until an adequate prototype is finally achieved from which the complete system or product can now be developed. Answer: C is incorrect. Rapid Application Development (RAD) refers to a type of software development methodology that uses minimal planning in favor of rapid prototyping.

QUESTION 157
Mark works as a Network Administrator for NetTech Inc. He wants users to access only those resources that are required for them. Which of the following access control models will he use?

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

Correct Answer: D
Section: Volume C

Explanation

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

QUESTION 158

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

Correct Answer: B
Section: Volume C

Explanation

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

QUESTION 159
Which of the following DITSCAP phases validates that the preceding work has produced an IS that operates in a specified computing environment?

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

Correct Answer: D
Section: Volume C

Explanation

Explanation/Reference:
Explanation: The Phase 3 of DITSCAP C&A is known as Validation. The goal of Phase 3 is to validate that the preceding work has produced an IS that operates in a specified computing environment. Answer: C is incorrect. 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: A is incorrect. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. Answer: B is incorrect. This phase ensures that it will maintain an acceptable level of residual risk.

QUESTION 160
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)

Correct Answer: A
Section: Volume C

Explanation

Explanation/Reference:
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).

QUESTION 161
Which of the following terms refers to a mechanism which proves that the sender really sent a particular message?

A. Confidentiality
B. Non-repudiation
C. Authentication

D. Integrity

Correct Answer: B
Section: Volume C

Explanation

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

QUESTION 162
In which of the following levels of exception safety are operations succeeded with full guarantee and fulfill all needs in the presence of exceptional situations?

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

Correct Answer: C
Section: Volume C

Explanation

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

QUESTION 163
Which of the following DoD policies establishes policies and assigns responsibilities to achieve DoD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network-centric warfare?

A. DoDI 5200.40
B. DoD 8500.1 Information Assurance (IA)
C. DoD 8510.1-M DITSCAP
D. DoD 8500.2 Information Assurance Implementation

Correct Answer: B
Section: Volume C

Explanation

Explanation/Reference:
Explanation: DoD 8500.1 Information Assurance (IA) sets up policies and allots responsibilities to achieve DoD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network-centric warfare. DoD 8500.1 also summarizes the roles and responsibilities for the persons responsible for carrying out the IA policies. Answer: D is incorrect. The DoD 8500.2 Information Assurance Implementation pursues 8500.1. It provides assistance on how to implement policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks. DoD Instruction 8500.2 allots tasks and sets procedures for applying integrated layered protection of the DOD information systems and networks in accordance with the DoD 8500.1 policy. It also provides some important guidelines on how to implement an IA program. Answer: A is incorrect. DoDI 5200.40 executes the policy, assigns responsibilities, and recommends procedures under reference for Certification and Accreditation (C&A) of information technology (IT). Answer: C is incorrect. DoD 8510.1-M DITSCAP provides standardized activities leading to accreditation, and establishes a process and management baseline.

QUESTION 164
Single Loss Expectancy (SLE) represents an organization's loss from a single threat. Which of the following formulas best describes the Single Loss Expectancy (SLE)?

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

Correct Answer: A
Section: Volume C

Explanation

Explanation/Reference:
Explanation: Single Loss Expectancy is a term related to Risk Management and Risk Assessment. It can be defined as the monetary value expected from the occurrence of a risk on an asset. It is mathematically expressed as follows: Single Loss Expectancy (SLE) = Asset Value (AV) * Exposure Factor (EF) where the Exposure Factor is represented in the impact of the risk over the asset, or percentage of asset lost. As an example, if the Asset Value is reduced two thirds, the exposure factor value is .66. If the asset is completely lost, the Exposure Factor is 1.0. The result is a monetary value in the same unit as the Single Loss Expectancy is expressed. Answer: C, D, and B are incorrect. These are not valid formulas of SLE.

QUESTION 165

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

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

Correct Answer: C
Section: Volume C

Explanation

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

QUESTION 166
SIMULATION
Fill in the blank with an appropriate security type. applies the internal security policies of the software applications when they are deployed.

Correct Answer: Programmatic security
Section: Volume C
Explanation

Explanation/Reference:
Explanation: Programmatic security applies the internal security policies of the software applications when they are deployed. In this type of security, the code of the software application controls the security behavior, and authentication decisions are made based on the business logic, such as the user role or the task performed by the user in a specific security context.

QUESTION 167
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

Correct Answer: C
Section: Volume C

Explanation

Explanation/Reference:
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 data. Answer: A is incorrect. The Continuity Of Operation Plan (COOP) refers to the preparations and institutions maintained by the United States government, providing survival of federal government operations in the case of catastrophic events. It provides procedures and capabilities to sustain an organization's essential. COOP is the procedure documented to ensure persistent critical operations throughout any period where normal operations are unattainable. 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.

QUESTION 168

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

Correct Answer: A
Section: Volume C

Explanation

Explanation/Reference:
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: C is incorrect. The Service Level Requirements document contains the requirements for a service from the client viewpoint, defining detailed service level targets, mutual responsibilities, and other requirements specific to a certain group of customers. Answer: D is incorrect. Underpinning Contract (UC) is a contract between an IT service provider and a third party. In another way, it is an agreement between the IT organization and an external provider about the delivery of one or more services. The third party provides services that support the delivery of a service to a customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level targets in an SLA.

QUESTION 169
Which of the following are the basic characteristics of declarative security? Each correct answer represents a complete solution. Choose all that apply.

A. It is a container-managed security.

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

Correct Answer: ABC

Section: Volume C
Explanation

Explanation/Reference:
Explanation: The following are the basic characteristics of declarative security: In declarative security, programming is not required. All security constraints are stated in the configuration files. It is a container-managed security. The application server manages the enforcing process of security constraints. It has a runtime environment. The security policies for runtime environment are represented by the deployment descriptor. It can support different environments, such as development, testing, and production. Answer: D is incorrect. It is the characteristic of programmatic security.

QUESTION 170
"Enhancing the Development Life Cycle to Produce Secure Software" summarizes the tools and practices that are helpful in producing secure software. What are these tools and practices? Each correct answer represents a complete solution. Choose three.

A. Leverage attack patterns
B. Compiler security checking and enforcement
C. Tools to detect memory violations
D. Safe software libraries E. Code for reuse and maintainability

Correct Answer: BCD
Section: Volume C
Explanation

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

QUESTION 171
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

Correct Answer: BCD
Section: Volume C
Explanation

Explanation/Reference:
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.

QUESTION 172
Which of the following NIST documents provides a guideline for identifying an information system as a National Security System?

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

Correct Answer: B
Section: Volume C

Explanation

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

QUESTION 173
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

Correct Answer: D
Section: Volume C

Explanation

Explanation/Reference:
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.

QUESTION 174
An authentication method uses smart cards as well as usernames and passwords for authentication. Which of the following authentication methods is being referred to?

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

Correct Answer: C
Section: Volume C

Explanation

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

create a user account in IIS to enable the user to connect anonymously. Answer: D is incorrect. Biometrics authentication uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user.

QUESTION 175
You work as a security engineer for BlueWell Inc. You want to use some techniques and procedures to verify the effectiveness of security controls in Federal Information System. Which of the following NIST documents will guide you?

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

Correct Answer: C
Section: Volume C

Explanation

Explanation/Reference:
Explanation: NIST has developed a suite of documents for conducting Certification & Accreditation (C&A). These documents are as follows: 1.NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems. 2.NIST Special Publication 800-53: This document provides a guideline for security controls for Federal Information Systems. 3.NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System. 4.NIST Special Publication 800-59: This document provides a guideline for identifying an information system as a National Security System. 5.NIST Special Publication 800-60: This document is a guide for mapping types of information and information systems to security objectives and risk levels.

QUESTION 176
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

Correct Answer: C
Section: Volume C

Explanation

Explanation/Reference:
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 data. Answer: D is incorrect. The network security policy is related to the security of a company's network. Answer: B is incorrect. The user password policy is related to passwords that users provide to log on to the network.

QUESTION 177
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

Correct Answer: C
Section: Volume C

Explanation

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

QUESTION 178
In which of the following IDS evasion attacks does an attacker send a data packet such that IDS accepts the data packet but the host computer rejects it?

A. Evasion attack
B. Fragmentation overlap attack
C. Fragmentation overwrite attack

D. Insertion attack

Correct Answer: D
Section: Volume C

Explanation

Explanation/Reference:
Explanation: 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. In this approach, an attacker sends packets in such a manner that one packet fragment overlaps data from a previous fragment. The information is organized in the packets in such a manner that when the victim's computer reassembles the packets, an attack string is executed on the victim's computer. Since the attacking string is in fragmented form, IDS is unable to detect it. Answer: C is incorrect. In this approach, an attacker sends packets in such a manner that one packet fragment overwrites data from a previous fragment. The information is organized into the packets in such a manner that when the victim's computer reassembles the packets, an attack string is executed on the victim's computer. Since the attacking string is in fragmented form, IDS becomes unable to detect it. Answer: A 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.

QUESTION 179
A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. What are the different types of policies? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: ACD
Section: Volume C
Explanation

Explanation/Reference:
Explanation: Following are the different types of policies: Regulatory: This type of policy ensures that the organization is following standards set by specific industry regulations. This policy type is very detailed and specific to a type of industry. This is used in financial institutions, health care facilities, public utilities, and other government-regulated industries, e.g., TRAI. Advisory: This type of policy strongly advises employees regarding which types of behaviors and activities should and should not take place within the organization. It also outlines possible ramifications if employees do not comply with the established behaviors and activities. This policy type can be used, for example, to describe how to handle medical information, handle financial transactions, or process confidential information. Informative:

This type of policy informs employees of certain topics. It is not an enforceable policy, but rather one to teach individuals about specific issues relevant to the company. It could explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations. Answer: B is incorrect. No such type of policy exists.

QUESTION 180
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

Correct Answer: ABD
Section: Volume C
Explanation

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

QUESTION 181
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

Correct Answer: D
Section: Volume C

Explanation

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

QUESTION 182
To help review or design security controls, they can be classified by several criteria. One of these criteria is based on time. According to this criteria, which of the following controls are intended to prevent an incident from occurring?

A. Corrective controls
B. Adaptive controls
C. Detective controls D. Preventive controls

Correct Answer: D
Section: Volume C

Explanation

Explanation/Reference:
Explanation: Preventive controls are the security controls that are intended to prevent an incident from occurring, e.g., by locking out unauthorized intruders. Answer: C is incorrect. Detective controls are intended to identify and characterize an incident in progress, e.g., by sounding the intruder alarm and alerting the security guards or police. Answer: A is incorrect. Corrective controls are intended to limit the extent of any damage caused by the incident, e.g., by recovering the organization to normal working status as efficiently as possible. Answer: B is incorrect. There is no such categorization of controls based on time.

QUESTION 183
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

Correct Answer: BCD
Section: Volume C
Explanation

Explanation/Reference:
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.

QUESTION 184
Which of the following NIST Special Publication documents provides a guideline on questionnaires and checklists through which systems can be evaluated for compliance against specific control objectives?

A. NIST SP 800-37
B. NIST SP 800-26
C. NIST SP 800-53A
D. NIST SP 800-59
E. NIST SP 800-53
F. NIST SP 800-60

Correct Answer: B
Section: Volume C

Explanation

Explanation/Reference:
Explanation: NIST SP 800-26 (Security Self-Assessment Guide for Information Technology Systems) provides a guideline on questionnaires and checklists through which systems can be evaluated for compliance against specific control objectives. Answer: A, E, C, D, and F are incorrect. NIST has developed a suite of documents for conducting Certification & Accreditation (C&A). These documents are as follows:
NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems. NIST Special Publication 800-53: This document provides a guideline for security controls for Federal Information Systems. NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System. NIST Special Publication 800-59: This document is a guideline for identifying an information system as a National Security System. NIST Special Publication 800-60: This document is a guide for mapping types of information and information systems to security objectives and risk levels.

QUESTION 185
A number of security patterns for Web applications under the DARPA contract have been developed by Kienzle, Elder, Tyree, and Edwards-Hewitt. Which of the following patterns are applicable to aspects of authentication in Web applications?b Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: ADEF
Section: Volume C
Explanation

Explanation/Reference:
Explanation: The various patterns applicable to aspects of authentication in the Web applications are as follows: Account lockout: It implements a limit on the incorrect password attempts to protect an account from automated password-guessing attacks. Authenticated session: It allows a user to access more than one access-restricted Web page without re-authenticating every page. It also integrates user authentication into the basic session model. Password authentication: It provides protection against weak passwords, automated password-guessing attacks, and mishandling of passwords. Password propagation: It offers a choice by requiring that a user's authentication credentials be verified by the database before providing access to that user's data. Answer: B and C are incorrect. Secure assertion and partitioned application patterns are applicable to software assurance in general.

QUESTION 186
Which of the following steps of the LeGrand Vulnerability-Oriented Risk Management method determines the necessary compliance offered by risk management practices and assessment of risk levels?

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

Correct Answer: A
Section: Volume C
Explanation

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

QUESTION 187

Which of the following security objectives are defined for information and information systems by the FISMA? Each correct answer represents a part of the solution. Choose all that apply.

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

Correct Answer: BCD
Section: Volume C
Explanation

Explanation/Reference:
Explanation: FISMA defines the following three security objectives for information and information systems: Confidentiality: It means that the data should only be accessible to authorized users. Access includes printing, displaying, and other such forms of disclosure, including simply revealing the existence of an object. Integrity: It means that only authorized users are able to modify data. Modification admits changing, changing the status, deleting, and creating. Availability: It means that the data should only be available to authorized users. Answer: A is incorrect. Authenticity is not defined by the FISMA as one of the security objectives for information and information systems.

QUESTION 188
Security Test and Evaluation (ST&E) is a component of risk assessment. It is useful in discovering system vulnerabilities. For what purposes is ST&E used? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: BCD
Section: Volume C
Explanation

Explanation/Reference:
Explanation: Security Test and Evaluation (ST&E) is a component of risk assessment. It is useful in discovering system vulnerabilities. According to NIST SP 80042 (Guideline on Network Security Testing), ST&E is used for the following purposes: To assess the degree of consistency between the system documentation and its implementation To determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy To uncover design, implementation, and operational flaws that may allow the violation of security policy Answer: A is incorrect. ST&E is not used for the implementation of the system architecture.

QUESTION 189
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.

Correct Answer: CD
Section: Volume C
Explanation

Explanation/Reference:
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.

QUESTION 190
A part of a project deals with the hardware work. As a project manager, you have decided to hire a company to deal with all hardware work on the project. Which type of risk response is this?

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

Correct Answer: C
Section: Volume C

Explanation

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

QUESTION 191
You work as a security manager for BlueWell Inc. You are performing the external vulnerability testing, or penetration testing to get a better snapshot of your organization's security posture. Which of the following penetration testing techniques will you use for searching paper disposal areas for unshredded or otherwise improperly disposed-of reports?

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

Correct Answer: C
Section: Volume C

Explanation

Explanation/Reference:
Explanation: Dumpster diving technique is used for searching paper disposal areas for unshredded or otherwise improperly disposed-of reports. Answer: B is incorrect. In scanning and probing technique, various scanners, like a port scanner, can reveal information about a network's infrastructure and enable an intruder

A.
to access the network's unsecured ports. Answer: D is incorrect. Demon dialing technique automatically tests every phone line in an exchange to try to locate modems that are attached to the network. Answer: A is incorrect. In sniffing technique, protocol analyzer can be used to capture data packets that are later decoded to collect information such as passwords or infrastructure configurations.

QUESTION 192
Which of the following are the benefits of information classification for an organization? Each correct answer represents a complete solution. Choose two.

It helps reduce the Total Cost of Ownership (TCO).
B. It helps identify which protections apply to which information.
C. It helps identify which information is the most sensitive or vital to an organization.
D. It ensures that modifications are not made to data by unauthorized personnel or processes.

Correct Answer: BC
Section: Volume C
Explanation

Explanation/Reference:
Explanation: Following are the benefits of information classification for an organization: It helps identify which protections apply to which information. It helps identify which information is the most sensitive or vital to an organization. It supports the tenets of confidentiality, integrity, and availability as it pertains to data. Answer: D is incorrect. The concept of integrity ensures that modifications are not made to data by unauthorized personnel or processes. It also ensures that unauthorized modifications are not made to data by authorized personnel or processes. Answer: A is incorrect. Information classification cannot reduce the Total Cost of Ownership (TCO).

QUESTION 193
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.

Correct Answer: ABD
Section: Volume C
Explanation

Explanation/Reference:

A.
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: C is incorrect. A software interface hides the implementation details of the component.

QUESTION 194
Elizabeth is a project manager for her organization and she finds risk management to be very difficult for her to manage. She asks you, a lead project manager, at what stage in the project will risk management become easier. What answer best resolves the difficulty of risk management practices and the effort required?

Risk management only becomes easier when the project moves into project execution.
B. Risk management only becomes easier when the project is closed.
C. Risk management is an iterative process and never becomes easier. D.
Risk management only becomes easier the more often it is practiced.

Correct Answer: D
Section: Volume C

Explanation

Explanation/Reference:
Explanation: According to the PMBOK, "Like many things in project management, the more it is done the easier the practice becomes." Answer: B is incorrect. This answer is not the best choice for the project. Answer: A is incorrect. Risk management likely becomes more difficult in project execution that in other stages of the project. Answer: C is incorrect. Risk management does become easier the more often it is done.

QUESTION 195
Which of the following describes a residual risk as the risk remaining after a risk mitigation has occurred?

A. DIACAP
B. SSAA
C. DAA
D. ISSO

Correct Answer: A
Section: Volume C

Explanation

Explanation/Reference:

A.

Explanation: DIACAP describes a residual risk as the risk remaining after a risk mitigation has occurred. The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk. DIACAP replaced the former process, known as DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process), in 2006. DoD Instruction (DoDI) 8510.01 establishes a standard DoD-wide process with a set of activities, general tasks, and a management structure to certify and accredit an Automated Information System (AIS) that will maintain the Information Assurance (IA) posture of the Defense Information Infrastructure (DII) throughout the system's life cycle.DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. It identifies four phases: 1.System Definition 2.Verification 3.Validation 4.Re-Accreditation Answer: D is incorrect. An Information System Security Officer (ISSO) plays the role of a supporter. The responsibilities of an Information System Security Officer (ISSO) are as follows: Manages the security of the information system that is slated for Certification & Accreditation (C&A). Insures the information systems configuration with the agency's information security policy. Supports the information system owner/information owner for the completion of security-related responsibilities. Takes part in the formal configuration management process. Prepares Certification & Accreditation (C&A) packages. Answer: C is incorrect. The Designated Approving Authority (DAA), in the United States Department of Defense, is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. The DAA is responsible for implementing system security. The DAA can grant the accreditation and can determine that the system's risks are not at an acceptable level

and the system is not ready to be operational. Answer: B 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.

QUESTION 196
You work as a Security Manager for Tech Perfect Inc. You want to save all the data from the SQL injection attack, which can read sensitive data from the database and modify database data using some commands, such as Insert, Update, and Delete. Which of the following tasks will you perform? Each correct answer represents a complete solution. Choose three.

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

Correct Answer: BCD
Section: Volume C
Explanation

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

QUESTION 197
Security is a state of well-being of information and infrastructures in which the possibilities of successful yet undetected theft, tampering, and/or disruption of information and services are kept low or tolerable. Which of the following are the elements of security? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: ABCD

Section: Volume C
Explanation

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

QUESTION 198
Harry is the project manager of the MMQ Construction Project. In this project, Harry has identified a supplier who can create stained glass windows for 1,000 window units in the construction project. The supplier is an artist who works by himself, but creates windows for several companies throughout the United States. Management reviews the proposal to use this supplier and while they agree that the supplier is talented, they do not think the artist can fulfill the 1,000 window units in time for the project's deadline. Management asked Harry to find a supplier who can fulfill the completion of the windows by the needed date in the schedule. What risk response has management asked Harry to implement?

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

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
Explanation: This is an example of mitigation. By changing to a more reliable supplier, Harry is reducing the probability the supplier will be late. It's still possible that the vendor may not be able to deliver the stained glass windows, but the more reputable supplier reduces the probability of the lateness. 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. Transference is when the risk is transferred to a third party, usually for a fee. While this question does include a contractual relationship, the risk is the lateness of the windows. Transference focuses on transferring the risk to a third party to manage the risk event. In this instance, the management of the risk is owned by a third party; the third party actually creates the risk event because of the possibility of the lateness of the windows. Answer: B is incorrect. Avoidance changes the project plan to avoid the risk. If the project manager and management changed the window-type to a standard window in the project requirements, then this would be avoidance. Risk avoidance is a technique used for threats. It creates changes to the project management plan that are meant to either eliminate the risk completely or to protect the project objectives from its impact. Risk avoidance removes the risk event entirely either by adding additional steps to avoid the event or reducing the project scope requirements. It may seem the answer to all possible risks, but avoiding risks also means losing out on the potential gains that accepting (retaining) the risk might have allowed. Answer: D is incorrect. Acceptance accepts the risk that the windows could be late and offers no response.

QUESTION 199
Which of the following refers to the ability to ensure that the data is not modified or tampered with?

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

Correct Answer: A
Section: Volume C

Explanation

Explanation/Reference:
Explanation: Integrity refers to the ability to ensure that the data is not modified or tampered with. Integrity means that data cannot be modified without authorization.
Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a Web site, when someone is able to cast a very large number of votes in an online poll, and so on. Answer: D is incorrect. Confidentiality is the property of preventing disclosure of information to unauthorized individuals or systems. Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Answer: B is incorrect. Availability means that data must be available whenever it is needed. Answer: C is incorrect. Nonrepudiation is the concept of ensuring that a party in a dispute cannot refuse to acknowledge, or refute the validity of a statement or contract. As a service, it provides proof of the integrity and origin of data. Although this concept can be applied to any transmission, including television and radio, by far the most common application is in the verification and trust of signatures.

QUESTION 200
The Phase 2 of DITSCAP C&A is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. What are the process activities of this phase? Each correct answer represents a complete solution. Choose all that apply.

A. Certification analysis
B. Assessment of the Analysis Results
C. Configuring refinement of the SSAA
D. System development
E. Registration

Correct Answer: ABCD

Section: Volume C
Explanation

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

QUESTION 201
Which of the following elements sets up a requirement to receive the constrained requests over a protected layer connection, such as TLS (Transport Layer Security)?

A. User data constraint
B. Authorization constraint
C. Web resource collection
D. Accounting constraint

Correct Answer: A
Section: Volume C

Explanation

Explanation/Reference:
Explanation: User data constraint is a security constraint element summarized in the Java Servlet Specification 2.4. It sets up a requirement to receive the constrained requests over a protected layer connection, such as TLS (Transport Layer Security). The user data constraint offers guarantee (NONE, INTEGRAL, and CONFEDENTIAL) for the transportation of data between client and server. If a request does not have user data constraint, the container accepts the request after it is received on a connection. Answer: C is incorrect. Web resource collection is a set of URL patterns and HTTP operations that define all resources required to be protected. It is a security constraint element summarized in the Java Servlet Specification v2.4. The Web resource collection includes the following elements: URL patterns HTTP methods Answer: B is incorrect. Authorization constraint is a security constraint element summarized in the Java Servlet Specification 2.4. It sets up a requirement for authentication and names the authorization roles that can access the URL patterns and HTTP methods as defined by the security constraint. In the absence of a security constraint, the container accepts the request without requiring any user authentication. If no authorization role is specified in the authorization constraint, the container cannot access constrained requests. The wildcard character "*" specifies all authorization role names that are defined in the deployment descriptor. Answer: D is incorrect. It is not a security constraint element.

QUESTION 202
In digital rights management, the level of robustness depends on the various types of tools and attacks to which they must be resistant or immune. Which of the following types of tools are expensive, require skill, and are not easily available?

A. Hand tools
B. Widely available tools
C. Specialized tools
D. Professional tools

Correct Answer: D
Section: Volume C

Explanation

Explanation/Reference:
Explanation: The tools used in DRM to define the level of robustness are as follows: 1.Widely available tools: These tools are easy to use and are available to everyone. For example, screw-drivers and file editors. 2.Specialized tools: These tools require skill and are available at reasonable prices. For example, debuggers, decompilers, and memory scanners. 3.Professional tools: These tools are expensive, require skill, and are not easily available. For example, logic analyzers, circuit emulators, and chip disassembly systems.

QUESTION 203
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

Correct Answer: ABD

Section: Volume C
Explanation

Explanation/Reference:
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: C is incorrect. No such type of NIACAP accreditation exists.

QUESTION 204
Which of the following statements about the integrity concept of information security management are true? Each correct answer represents a complete solution. Choose three.

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

Correct Answer: ACD
Section: Volume C
Explanation

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

QUESTION 205
Which of the following are the important areas addressed by a software system's security policy? Each correct answer represents a complete solution. Choose all that apply.

A. Identification and authentication
B. Punctuality
C. Data protection
D. Accountability
E. Scalability

F. Access control

Correct Answer: ACDF
Section: Volume C
Explanation

Explanation/Reference:
Explanation: The security policy of a software system addresses the following important areas: Access control Data protection Confidentiality Integrity Identification and authentication Communication security Accountability Answer: E and B are incorrect. Scalability and punctuality are not addressed by a software system's security policy.

QUESTION 206
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

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:
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: C 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.

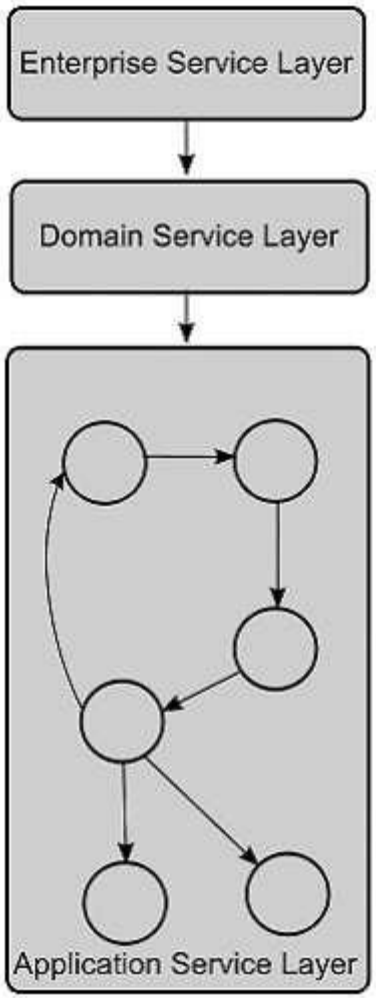
QUESTION 207
Which of the following security architectures defines how to integrate widely disparate applications for a world that is Web-based and uses multiple implementation platforms?

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

Correct Answer: C
Section: Volume C

Explanation

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



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

supporting SOA. Answer: B is incorrect. Enterprise architecture describes the terminology, the composition of subsystems, and their relationships with the external environment, and the guiding principles for the design and evolution of an enterprise.

QUESTION 208
Which of the following recovery plans includes specific strategies and actions to deal with specific variances to assumptions resulting in a particular security problem, emergency, or state of affairs?

A. Disaster recovery plan
B. Business continuity plan
C. Continuity of Operations Plan
D. Contingency plan

Correct Answer: D
Section: Volume C

Explanation

Explanation/Reference:
Explanation: A contingency plan is a plan devised for a specific situation when things could go wrong. 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. Answer: A is incorrect. Disaster recovery is the process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Answer: B is incorrect. It deals with the plans and procedures that identify and prioritize the critical business functions that must be preserved. Answer: C is incorrect. It includes the plans and procedures documented that ensure the continuity of critical operations during any period where normal operations are impossible.

QUESTION 209
The mission and business process level is the Tier 2. What are the various Tier 2 activities? Each correct answer represents a complete solution. Choose all that apply.

A. Developing an organization-wide information protection strategy and incorporating high-level information security requirements
B. Defining the types of information that the organization needs, to successfully execute the stated missions and business processes
C. Specifying the degree of autonomy for the subordinate organizations
D. Defining the core missions and business processes for the organization
E. Prioritizing missions and business processes with respect to the goals and objectives of the organization

Correct Answer: ABCDE
Section: Volume C
Explanation

Explanation/Reference:
Explanation: The mission and business process level is the Tier 2. It addresses risks from the mission and business process perspective. It is guided by the risk decisions at Tier 1. The various Tier 2 activities are as follows: It defines the core missions and business processes for the organization. It also prioritizes missions and business processes, with respect to the goals and objectives of the organization. It defines the types of information that an organization requires, to successfully execute the stated missions and business processes. It helps in developing an organization-wide information protection strategy and incorporating high-level information security requirements. It specifies the degree of autonomy for the subordinate organizations.

QUESTION 210
You are responsible for network and information security at a metropolitan police station. The most important concern is that unauthorized parties are not able to access data. What is this called?

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

Correct Answer: A
Section: Volume C

Explanation

Explanation/Reference:
Explanation: The CIA (Confidentiality, Integrity, and Availability) triangle is concerned with three facets of security. Confidentiality is the concern that data be secure from unauthorized access. Answer: B and C are incorrect. The CIA (Confidentiality, Integrity, and Availability) triangle is concerned with three facets of security. Integrity is the concern that data not be altered without it being traceable. Availability is the concern that the data, while being secured, is readily accessible. Answer: D is incorrect. Confidentiality may be implemented with encryption but encryption is just a technique to obtain confidentiality.

QUESTION 211
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

Correct Answer: C
Section: Volume C

Explanation

Explanation/Reference:
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.

QUESTION 212
Which of the following is NOT a responsibility of a data owner?

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

Correct Answer: D
Section: Volume C

Explanation

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

QUESTION 213
ISO 27003 is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Which of the following elements does this standard contain? Each correct answer represents a complete solution. Choose all that apply.

A. Inter-Organization Co-operation
B. Information Security Risk Treatment
C. CSFs (Critical success factors)
D. ystem requirements for certification bodies Managements
E. Terms and Definitions
F. Guidance on process approach

Correct Answer: ACEF
Section: Volume C
Explanation

Explanation/Reference:
Explanation: ISO 27003 is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is entitled as "Information Technology - Security techniques - Information security management system implementation guidance". The ISO 27003 standard provides guidelines for implementing an ISMS (Information Security Management System). It mainly focuses upon the PDCA method along with establishing, implementing, reviewing, and improving the ISMS itself. The ISO 27003 standard contains the following elements: Introduction Scope Terms and Definitions CSFs (Critical success factors) Guidance on process approach Guidance on using PDCA Guidance on Plan Processes Guidance on Do Processes Guidance on Check Processes Guidance on Act Processes Inter-Organization Co-operation Answer: B is incorrect. This element is included in the ISO 27005 standard. Answer: D is incorrect. This element is included in the ISO 27006 standard.

QUESTION 214
John works as a security manager for SoftTech Inc. He is working with his team on the disaster recovery management plan. One of his team members has a doubt related to the most cost effective DRP testing plan. According to you, which of the following disaster recovery testing plans is the most cost-effective and efficient way to identify areas of overlap in the plan before conducting more demanding training exercises?

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

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
Explanation: The structured walk-through test is also known as the table-top exercise. In structured walk-through test, the team members walkthrough the plan to identify and correct weaknesses and how they will respond to the emergency scenarios by stepping in the course of the plan. It is the most effective and competent

way to identify the areas of overlap in the plan before conducting more challenging training exercises. Answer: A is incorrect. In full-scale exercise, the critical systems run at an alternate site. Answer: B is incorrect. The emergency management group and response teams actually perform their emergency response functions by walking through the test, without actually initiating recovery procedures. But it is not much cost effective. Answer: D is incorrect. It is a test performed when personnel walks through the evacuation route to a designated area where procedures for accounting for the personnel are tested.

QUESTION 215
Which of the following statements describe the main purposes of a Regulatory policy? Each correct answer represents a complete solution. Choose all that apply.

A. It acknowledges the importance of the computing resources to the business model
B. It provides a statement of support for information security throughout the enterprise
C. It ensures that an organization is following the standard procedures or base practices of operation in its specific industry.
D. It gives an organization the confidence that it is following the standard and accepted industry policy.

Correct Answer: CD
Section: Volume C
Explanation

Explanation/Reference:
Explanation: The main purposes of a Regulatory policy are as follows: It ensures that an organization is following the standard procedures or base practices of operation in its specific industry. It gives an organization the confidence that it is following the standard and accepted industry policy. Answer: B and A are incorrect. These are the policy elements of Senior Management Statement of Policy.

QUESTION 216
Audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function. Under which of the following controls does audit control come?

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

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:
Explanation: Audit trail or audit log comes under detective controls. Detective controls are the audit controls that are not needed to be restricted. Any control that performs a monitoring activity can likely be defined as a Detective Control. For example, it is possible that mistakes, either intentional or unintentional, can be made. Therefore, an additional Protective control is that these companies must have their financial results audited by an independent Certified Public Accountant. The role of this accountant is to act as an auditor. In fact, any auditor acts as a Detective control. If the organization in question has not properly followed the rules,

a diligent auditor should be able to detect the deficiency which indicates that some control somewhere has failed. Answer: A is incorrect. Reactive or corrective controls typically work in response to a detective control, responding in such a way as to alert or otherwise correct an unacceptable condition. Using the example of account rules, either the internal Audit Committee or the SEC itself, based on the report generated by the external auditor, will take some corrective action. In this way, they are acting as a Corrective or Reactive control. Answer: C and D are incorrect. Protective or preventative controls serve to proactively define and possibly enforce acceptable behaviors. As an example, a set of common accounting rules are defined and must be followed by any publicly traded company. Each quarter, any particular company must publicly state its current financial standing and accounting as reflected by an application of these rules. These accounting rules and the SEC requirements serve as protective or preventative controls.

QUESTION 217

Which of the following is generally used in packages in order to determine the package or product tampering?

A. Tamper resistance
B. Tamper evident
C. Tamper data
D. Tamper proof

Correct Answer: A
Section: Volume C

Explanation

Explanation/Reference:

Explanation: Tamper resistance is resistance tampered by the users of a product, package, or system, or the users who can physically access it. It includes simple as well as complex devices. The complex device encrypts all the information between individual chips, or renders itself inoperable. Tamper resistance is generally used in packages in order to determine package or product tampering. Answer: B is incorrect. Tamper evident specifies a process or device that makes unauthorized access to the protected object easily detected. Answer: D is incorrect. Tamper proofing makes computers resistant to interference. Tamper proofing measures include automatic removal of sensitive information, automatic shutdown, and automatic physical locking. Answer: C is incorrect. Tamper data is used to view and modify the HTTP or HTTPS headers and post parameters.

QUESTION 218

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

Correct Answer: D
Section: Volume C

Explanation

Explanation/Reference:
Explanation: Graybox testing is a combination of whitebox testing and blackbox testing. In graybox testing, the test engineer is equipped with the knowledge of system and designs test cases or test data based on system knowledge. The security tester typically performs graybox testing to find vulnerabilities in software and network system. Answer: C 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.

QUESTION 219
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

Correct Answer: B
Section: Volume C

Explanation

Explanation/Reference:
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: C 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.

QUESTION 220
Which of the following approaches can be used to build a security program? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: CD
Section: Volume C
Explanation

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