ISC2

Exam Questions CSSLP

Certified Information Systems Security Professional

NEW QUESTION 1
Which of the following are the common roles with regard to data in an information classification program? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BCDE

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

NEW QUESTION 2
Joseph works as a Software Developer for WebTech Inc. He wants to protect the algorithms and the techniques of programming that he uses in developing an application. Which of the following laws are used to protect a part of software?

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

Answer: B

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

NEW QUESTION 3
Which of the following is a signature-based intrusion detection system (IDS) ?

A. RealSecure
B. StealthWatch
C. Tripwire
D. Snort

Answer: D

Explanation:
Snort is a signature-based intrusion detection system. 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 user-defined rule set. Answer B is incorrect. StealthWatch is a behavior-based intrusion detection system. Answer A is incorrect. RealSecure is a network-based IDS that monitors TCP, UDP and ICMP traffic and is configured to look for attack patterns. Answer C is incorrect. Tripwire is a file integrity checker for UNIX/Linux that can be used for host-based intrusion detection.

NEW QUESTION 4
In which of the following types of tests are the disaster recovery checklists distributed to the members of disaster recovery team and asked to review the assigned checklist?

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

Answer: D

Explanation:
A checklist test is a test in which the disaster recovery checklists are distributed to the members of the disaster recovery team. All members are asked to review the assigned checklist. The checklist test is a simple test and it is easy to conduct this test. It allows to accomplish the following three goals: It ensures that the employees are aware of their responsibilities and they have the refreshed knowledge. It provides an individual with an opportunity to review the checklists for obsolete information and update any items that require modification during the changes in the organization. It ensures that the assigned members of disaster recovery team are still working for the organization. Answer B is incorrect. A simulation test is a method used to test the disaster recovery plans. It operates just like a structured walk- through test. In the simulation test, the members of a disaster recovery team present with a disaster scenario and then, discuss on appropriate responses. These suggested responses are measured and some of them are taken by the team. The range of the simulation test should be defined carefully for avoiding excessive disruption of normal business activities. Answer A is incorrect. A parallel test includes the next level in the testing procedure, and

relocates the employees to an alternate recovery site and implements site activation procedures. These employees present with their disaster recovery responsibilities as they would for an actual disaster. The disaster recovery sites have full responsibilities to conduct the day-to-day organization's business. Answer C is incorrect. A full-interruption test includes the operations that shut down at the primary site and are shifted to the recovery site according to the disaster recovery plan. It operates just like a parallel test. The full-interruption test is very expensive and difficult to arrange. Sometimes, it causes a major disruption of operations if the test fails.

NEW QUESTION 5
You are the project manager of the CUL project in your organization. You and the project team are assessing the risk events and creating a probability and impact matrix for the identified risks. Which one of the following statements best describes the requirements for the data type used in qualitative risk analysis?

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

Answer: C

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

NEW QUESTION 6
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()

Answer: A

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

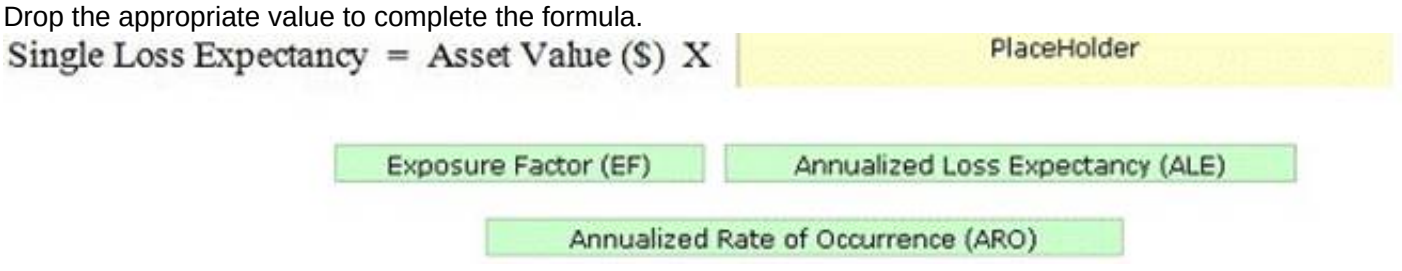
NEW QUESTION 7
What are the various activities performed in the planning phase of the Software Assurance Acquisition process? Each correct answer represents a complete solution. Choose all that apply.

A. Develop software requirements.
B. Implement change control procedures.
C. Develop evaluation criteria and evaluation plan.
D. Create acquisition strategy.

Answer: ACD

Explanation:
The various activities performed in the planning phase of the Software Assurance Acquisition process are as follows: Determine software product or service requirements. Identify associated risks. Develop software requirements. Create acquisition strategy. Develop evaluation criteria and evaluation plan. Define development and use of SwA due diligence questionnaires. Answer B is incorrect. This activity is performed in the monitoring and acceptance phase of the Software Assurance acquisition process.

NEW QUESTION 8
DRAG DROP
Drop the appropriate value to complete the formula.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
A Single Loss Expectancy (SLE) is the value in dollar ($) that is assigned to a single event. The SLE can be calculated by the following formula: SLE = Asset Value ($) X Exposure Factor (EF) The Exposure Factor (EF) represents the % of assets loss caused by a threat. The EF is required to calculate the Single Loss

Expectancy (SLE). The Annualized Loss Expectancy (ALE) 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.

NEW QUESTION 9
Which of the following governance bodies directs and coordinates implementations of the information security program?

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

Answer: A

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

Governance Body	Membership	Responsibilities
Information Security Steering 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.

NEW QUESTION 10
The IAM/CA makes certification accreditation recommendations to the DAA. The DAA issues accreditation determinations. Which of the following are the accreditation determinations issued by the DAA? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABCD

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

NEW QUESTION 10
In which of the following testing methodologies do assessors use all available documentation and work under no constraints, and attempt to circumvent the security features of an information system?

A. Full operational test
B. Penetration test
C. Paper test
D. Walk-through test

Answer: B

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

NEW QUESTION 14
The Phase 4 of DITSCAP C&A is known as Post Accreditation. This phase starts after the system has been accredited in Phase 3. What are the process activities of this phase? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABCDE

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

NEW QUESTION 15
Bill is the project manager of the JKH Project. He and the project team have identified a risk event in the project with a high probability of occurrence and the risk event has a high cost impact on the project. Bill discusses the risk event with Virginia, the primary project customer, and she decides that the requirements surrounding the risk event should be removed from the project. The removal of the requirements does affect the project scope, but it can release the project from the high risk exposure. What risk response has been enacted in this project?

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

Answer: D

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

NEW QUESTION 17
Which of the following process areas does the SSE-CMM define in the 'Project and Organizational Practices' category? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ACD

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

NEW QUESTION 22
Which of the following security design patterns provides an alternative by requiring that a user's authentication credentials be verified by the database before providing access to that user's data?

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

Answer: C

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

NEW QUESTION 27
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

Answer: B

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.

NEW QUESTION 28
Which of the following attacks causes software to fail and prevents the intended users from accessing software?

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

Answer: C

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

NEW QUESTION 29
You work as a Network Auditor for Net Perfect Inc. The company has a Windows-based network. While auditing the company's network, you are facing problems in searching the faults and other entities that belong to it. Which of the following risks may occur due to the existence of these problems?

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

Answer: C

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

NEW QUESTION 30
A Web-based credit card company had collected financial and personal details of Mark before issuing him a credit card. The company has now provided Mark's financial and personal details to another company. Which of the following Internet laws has the credit card issuing company violated?

A. Trademark law
B. Security law
C. Privacy law
D. Copyright law

Answer: C

Explanation:
The credit card issuing company has violated the Privacy law. According to the Internet Privacy law, a company cannot provide their customer's financial and personal details to other companies. Answer A is incorrect. Trademark laws facilitate the protection of trademarks around the world. Answer B is incorrect. There is no law such as Security law. Answer D is incorrect. The Copyright law protects original works or creations of authorship including literary, dramatic, musical, artistic, and certain other intellectual works.

NEW QUESTION 33
Della work as a project manager for BlueWell Inc. A threat with a dollar value of $250,000 is expected to happen in her project and the frequency of threat occurrence per year is 0.01. What will be the annualized loss expectancy in her project?

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

Answer: B

Explanation:
The annualized loss expectancy in her project will be $2,500. Annualized loss expectancy (ALE) is the annually expected financial loss to an organization from a threat. The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as follows: ALE = 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.

NEW QUESTION 38
Which of the following is a name, symbol, or slogan with which a product is identified?

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

Answer: A

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

NEW QUESTION 39
You work as a security engineer for BlueWell Inc. Which of the following documents will you use as a guide for the security certification and accreditation of Federal Information Systems?

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

Answer: C

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

NEW QUESTION 40
Which of the following penetration testing techniques automatically tests every phone line in an exchange and tries to locate modems that are attached to the network?

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

Answer: A

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

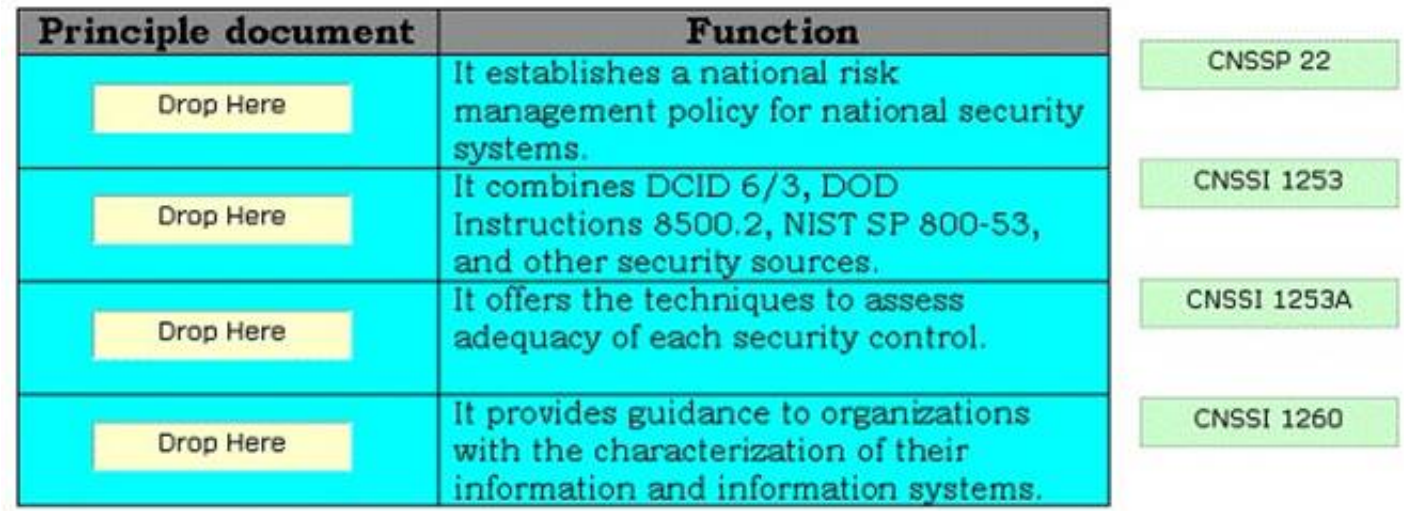
NEW QUESTION 42
Which of the following actions does the Data Loss Prevention (DLP) technology take when an agent detects a policy violation for data of all states? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABD

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

NEW QUESTION 46
DRAG DROPDrag and drop the appropriate principle documents in front of their respective functions.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
The various principle documents of transformation are as follows: CNSSP 22: It establishes a national risk management policy for national security systems. CNSSI 1199: It creates the technique in which the national security community classifies the information and information systems with regard to confidentiality, integrity, and availability. CNSSI 1253: It combines DCID 6/3, DOD Instructions 8500.2, NIST SP 800-53, and other security sources into a single cohesive repository of security controls. CNSSI 1253 A. It offers the
techniques to assess adequacy of each security control. CNSSI 1260: It provides guidance to organizations with the characterization of their information and information systems. NIST 800-37, Revision 1: It defines the certification and accreditation (C & A) process. The NIST 800-37, Revision 1 is a combination of DNI, DoD, and NIST.

NEW QUESTION 47
Which of the following types of activities can be audited for security? Each correct answer represents a complete solution. Choose three.

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

Answer: ACD

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

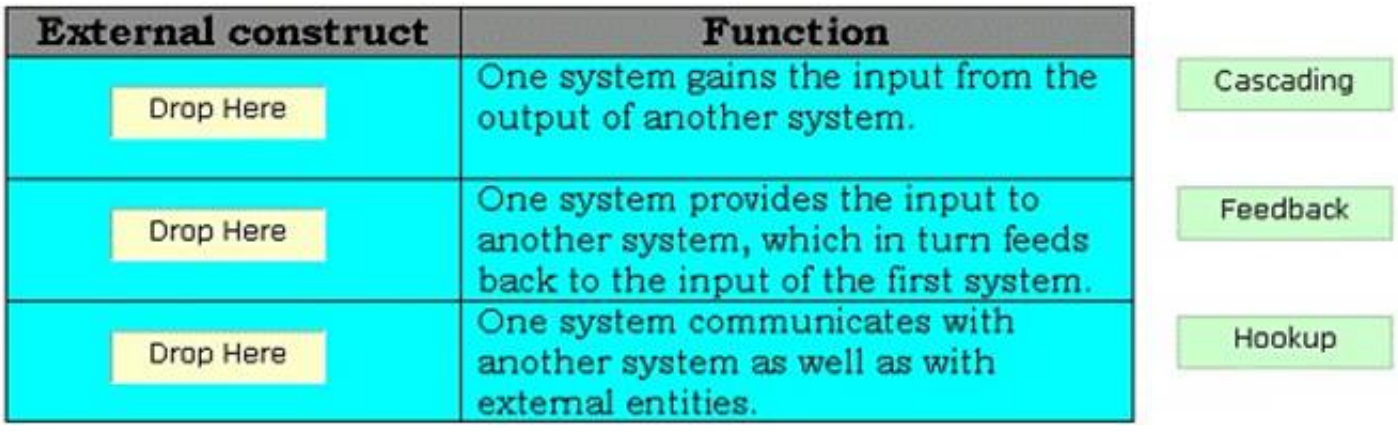
NEW QUESTION 49
The DoD 8500 policy series represents the Department's information assurance strategy. Which of the following objectives are defined by the DoD 8500 series? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ACD

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

NEW QUESTION 52
DRAG DROPDrag and drop the appropriate external constructs in front of their respective functions.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 55
Software Development Life Cycle (SDLC) is a logical process used by programmers to develop software. Which of the following SDLC phases meets the audit objectives defined below: System and data are validated. System meets all user requirements. System meets all control requirements.

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

Answer: A

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

NEW QUESTION 60
Which of the following agencies is responsible for funding the development of many technologies such as computer networking, as well as NLS?

A. DIAP
B. DTIC
C. DARPA
D. DISA

Answer: C

Explanation:
The Defense Advanced Research Projects Agency (DARPA) is an agency of the United States Department of Defense responsible for the development of new technology for use by the military. DARPA has been responsible for funding the development of many technologies which have had a major effect on the world, including computer networking, as well as NLS, which was both the first hypertext system, and an important precursor to the contemporary ubiquitous graphical user interface. DARPA supplies technological options for the entire Department, and is designed to be the "technological engine" for transforming DoD. Answer D is incorrect. The Defense Information Systems Agency is a United States Department of Defense combat support agency with the goal of providing real-time information technology (IT) and communications support to the President, Vice President, Secretary of Defense, the military Services, and the Combatant Commands. DISA, a Combat Support Agency, engineers and provides command and control capabilities and enterprise infrastructure to continuously operate and assure a global net-centric enterprise in direct support to joint warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations.
Answer B is incorrect. The Defense Technical Information Center (DTIC) is a repository of scientific and technical documents for the United States Department of Defense. DTIC serves the DoD community as the largest central resource for DoD and government-funded scientific, technical, engineering, and business related information available today. DTIC's documents are available to DoD personnel and defense contractors, with unclassified documents also available to the public. DTIC's aim is to serve a vital link in the transfer of information among DoD personnel, DoD contractors, and potential contractors and other U.S. Government agency personnel and their contractors. Answer A is incorrect. The Defense-wide Information Assurance Program (DIAP) protects and supports DoD information, information systems, and information networks, which is important to the Department and the armed forces throughout the day-to-day operations, and in the time of crisis. The DIAP uses the OSD method to plan, observe, organize, and incorporate IA activities. The role of DIAP is to act as a facilitator for program execution by the combatant commanders, Military Services, and Defense Agencies. The DIAP staff combines functional and programmatic skills for a comprehensive Defense-wide approach to IA. The DIAP's main objective is to ensure that the DoD's vital information resources are secured and protected by incorporating IA activities to get a secure net-centric GIG operation enablement and information supremacy by applying a Defense-in-Depth methodology that integrates the capabilities of people, operations, and technology to establish a multi-layer, multidimensional protection.

NEW QUESTION 65
Which of the following security issues does the Bell-La Padula model focus on?

A. Authorization

B. Confidentiality
C. Integrity
D. Authentication

Answer: B

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

NEW QUESTION 68
Numerous information security standards promote good security practices and define frameworks or systems to structure the analysis and design for managing information security controls. Which of the following are the international information security standards? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BCD

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

NEW QUESTION 69
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

Answer: B

Explanation:
Integrity ensures that no intentional or unintentional unauthorized modification is made to datAnswer D is incorrect. Confidentiality refers to the protection of data against unauthorized access. Administrators can provide confidentiality by encrypting datAnswer A is incorrect. Non-repudiation is a mechanism to prove that the sender really sent this message. Answer B is incorrect. Authentication is the process of verifying the identity of a person or network host.

NEW QUESTION 73
In which of the following architecture styles does a device receive input from connectors and generate transformed outputs?

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

Answer: C

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

NEW QUESTION 75
Which of the following features of SIEM products is used in analysis for identifying potential problems and reviewing all available data that are associated with the problems?

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

Answer: B

Explanation:

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

NEW QUESTION 77
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

Answer: C

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

NEW QUESTION 78
Which of the following vulnerabilities occurs when an application directly uses or concatenates potentially hostile input with data file or stream functions?

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

Answer: B

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

NEW QUESTION 79
Which of the following are the levels of public or commercial data classification system? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABDF

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

NEW QUESTION 84
An attacker exploits actual code of an application and uses a security hole to carry out an attack before the application vendor knows about the vulnerability. Which of the following types of attack is this?

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

Answer: B

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

the information to the receiving host. The receiving host responds to the software, presuming it to be the legitimate client. Answer D is incorrect. A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as network saturation attack or bandwidth consumption attack. Attackers perform DoS attacks by sending a large number of protocol packets to a network.

NEW QUESTION 85
Which of the following statements are true about declarative security? Each correct answer represents a complete solution. Choose all that apply.

A. It is employed in a layer that relies outside of the software code or uses attributes of the code.
B. It applies the security policies on the software applications at their runtime.
C. In this security, authentication decisions are made based on the business logic.
D. In this security, the security decisions are based on explicit statements.

Answer: ABD

Explanation:
Declarative security applies the security policies on the software applications at their runtime. In this type of security, the security decisions are based on explicit statements that confine security behavior. Declarative security applies security permissions that are required for the software application to access the local resources and provides role-based access control to an individual software component and software application. It is employed in a layer that relies outside of the software code or uses attributes of the code. Answer B is incorrect. In declarative security, authentication decisions are coarse- grained in nature from an operational or external security perspective.

NEW QUESTION 89
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

Answer: A

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

NEW 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

Answer: D

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

NEW QUESTION 98
At which of the following levels of robustness in DRM must the security functions be immune to widely available tools and specialized tools and resistant to professional tools?

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

Answer: C

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

NEW QUESTION 102
Which of the following requires all general support systems and major applications to be fully certified and accredited before these systems and applications are put into production? Each correct answer represents a part of the solution. Choose all that apply.

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

Answer:

BD

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

NEW QUESTION 107
Which of the following types of attacks occurs when an attacker successfully inserts an intermediary software or program between two communicating hosts?

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

Answer: C

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

NEW QUESTION 112
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

Answer: A

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 B is incorrect. It is not a valid type of policy.

NEW QUESTION 116
What are the security advantages of virtualization, as described in the NIST Information Security and Privacy Advisory Board (ISPAB) paper "Perspectives on Cloud Computing and Standards"? Each correct answer represents a complete solution. Choose three.

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

Answer: ABC

Explanation:
The security advantages of virtualization are as follows: It adds a layer of security for defense-in-depth. It provides strong encapsulation of errors. It increases intrusion detection through introspection. It decreases exposure of weak software. It increases the flexibility for discovery. It increases capabilities for fault tolerant computing using rollback and snapshot features. Answer D is incorrect. Virtualization increases configuration effort because of complexity of the virtualization layer and composite system.

NEW QUESTION 118
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

Answer: C

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.

NEW QUESTION 121
Which of the following strategies is used to minimize the effects of a disruptive event on a company, and is created to prevent interruptions to normal business activity?

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

Answer: D

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

NEW QUESTION 123
Which of the following tiers addresses risks from an information system perspective?

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

Answer: B

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

NEW QUESTION 125
Which of the following persons in an organization is responsible for rejecting or accepting the residual risk for a system?

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

Answer: B

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

NEW QUESTION 129
Which of the following sections come under the ISO/IEC 27002 standard?

A. Security policy
B. Asset management

C. Financial assessment
D. Risk assessment

Answer: ABD

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

NEW QUESTION 131
Which of the following provides an easy way to programmers for writing lower-risk applications and retrofitting security into an existing application?

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

Answer: D

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

NEW QUESTION 132
Continuous Monitoring is the fourth phase of the security certification and accreditation process. What activities are performed in the Continuous Monitoring process? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BDE

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

NEW QUESTION 136
DRAG DROP
Drag and drop the correct DoD Policy Series at their appropriate places.

Policy Subject Area	DoD Policy Series
General	Drop Here
IA Certification and Accreditation	Drop Here
Security Management	Drop Here
Computer Network Defense	Drop Here
IA Education, Training, and Awareness	Drop Here
Interconnectivity	Drop Here

8540
8570
8530
8520
8510
8500

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The various DoD policy series are as follows:

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

NEW QUESTION 137
Fill in the blank with an appropriate phrase. is used to provide security mechanisms for the storage, processing, and transfer of data.

A. Data classification

Answer: A

Explanation:
Data classification is used to protect the data based on its sensitivity, secrecy, and confidentiality. It provides security mechanisms for storage, processing, and transfer of data. Data classification also helps to verify the effort, funds, and resources allocated to save the data, and controls access to it.

NEW QUESTION 138
"Enhancing the Development Life Cycle to Produce Secure Software" summarizes the tools and practices that are helpful in producing secure software. What are these tools and practices? Each correct answer represents a complete solution. Choose three.

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

Answer: BCD

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

NEW QUESTION 139
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

Answer: C

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.

NEW QUESTION 144
You work as a system engineer for BlueWell Inc. You want to verify that the build meets its
data requirements, and correctly generates each expected display and report. Which of the following tests will help you to perform the above task?

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

Answer: B

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

NEW QUESTION 145
Which of the following processes identifies the threats that can impact the business continuity of operations?

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

Answer: C

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

NEW QUESTION 148
How can you calculate the Annualized Loss Expectancy (ALE) that may occur due to a threat?

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

Answer: A

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

NEW QUESTION 153
Certification and Accreditation (C&A or CnA) is a process for implementing information security. Which of the following is the correct order of C&A phases in a DITSCAP assessment?

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

Answer: C

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

NEW QUESTION 155
Copyright holders, content providers, and manufacturers use digital rights management (DRM) in order to limit usage of digital media and devices. Which of the following security challenges does DRM include? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ACD

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

NEW QUESTION 157
An authentication method uses smart cards as well as usernames and passwords for authentication. Which of the following authentication methods is being referred to?

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

Answer: C

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

NEW QUESTION 159
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

Answer: B

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.

NEW QUESTION 161
Which of the following NIST documents provides a guideline for identifying an information system as a National Security System?

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

Answer: B

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

NEW QUESTION 166
According to the NIST SAMATE, dynamic analysis tools operate by generating runtime vulnerability scenario using some functions. Which of the following are functions that are used by the dynamic analysis tools and are summarized in the NIST SAMATE? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ACD

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

NEW QUESTION 171
Which of the following allows multiple operating systems (guests) to run concurrently on a host computer?

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

Answer: B

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

NEW QUESTION 172
Which of the following disaster recovery tests includes the operations that shut down at the primary site, and are shifted to the recovery site according to the disaster recovery plan?

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

Answer: B

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

NEW QUESTION 173
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

Answer: BCD

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.

NEW QUESTION 177
Which of the following fields of management focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life?

A. Configuration management
B. Risk management
C. Change management
D. Procurement management

Answer: A

Explanation:

Configuration management is a field of management that focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life. Configuration Management System is a subsystem of the overall project management system. It is a collection of formal documented procedures used to identify and document the functional and physical characteristics of a product, result, service, or component of the project. It also controls any changes to such characteristics, and records and reports each change and its implementation status. It includes the documentation, tracking systems, and defined approval levels necessary for authorizing and controlling changes. Audits are performed as part of configuration management to determine if the requirements have been met. Answer D is incorrect. The procurement management plan defines more than just the procurement of team members, if needed. It defines how procurements will be planned and executed, and how the organization and the vendor will fulfill the terms of the contract. Answer B 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. Answer B is incorrect. Change Management is used to ensure that standardized methods and procedures are used for efficient handling of all changes.

NEW QUESTION 182
Which of the following can be used to accomplish authentication? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BCD

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

NEW QUESTION 184
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

Answer: C

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.

NEW QUESTION 189
Which of the following documents is defined as a source document, which is most useful for the ISSE when classifying the needed security functionality?

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

Answer: A

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

NEW QUESTION 193
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

Answer: D

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.

NEW QUESTION 194
Which of the following security related areas are used to protect the confidentiality, integrity, and availability of federal information systems and information processed by those systems?

A. Personnel security
B. Access control
C. Configuration management
D. Media protection
E. Risk assessment

Answer: ABCDE

Explanation:
The minimum security requirements cover seventeen security related areas to protect the confidentiality, integrity, and availability of federal information systems and information processed by those systems. They are as follows: Access control Awareness and training Audit and accountability Certification, accreditation, and security assessment Configuration management Contingency planning Identification and authentication Incident response Maintenance Media protection Physical and environmental protection Planning Personnel security Risk assessment Systems and services acquisition System and communications protection System and information integrity

NEW QUESTION 197
Which of the following is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known, but by which a business can obtain an economic advantage over its competitors?

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

Answer: C

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

NEW QUESTION 199
DRAG DROP
RCA (root cause analysis) is an iterative and reactive method that identifies the root cause of various incidents, and the actions required to prevent these incidents from reoccurring. RCA is classified in various categories. Choose appropriate categories and drop them in front of their respective functions.

RCA categories	Functions
Drop Here	It consists of plans from the health and safety areas.
Drop Here	It integrates quality control paradigms.
Drop Here	It integrates business processes.
Drop Here	It integrates failure analysis processes.
Drop Here	It integrates the methods from risk and systems analysis.

Safety-based RCA
Production-based RCA
Process-based RCA
Failure-based RCA
Systems-based RCA

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 201
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

Answer: BCDEF

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

NEW QUESTION 203
Which of the following classification levels defines the information that, if disclosed to the unauthorized parties, could be reasonably expected to cause exceptionally grave damage to the national security?

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

Answer: D

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

NEW QUESTION 208
Which of the following statements about a host-based intrusion prevention system (HIPS) are true? Each correct answer represents a complete solution. Choose two.

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

Answer: CD

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

NEW QUESTION 213
Fill in the blank with an appropriate phrase The is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity.

A. Biba model

Answer: A

Explanation:
The Biba model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject.

NEW QUESTION 218
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

Answer: B

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 B 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

NEW QUESTION 223
You are the project manager of the GHY project for your organization. You are about to start the qualitative risk analysis process for the project and you need to determine the roles and responsibilities for conducting risk management. Where can you find this information?

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

Answer: C

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

NEW QUESTION 225
Shoulder surfing is a type of in-person attack in which the attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard of an employee's computer while he is typing in his password at any access point such as a terminal/Web site. Which of the following is violated in a shoulder surfing attack?

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

Answer: C

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

NEW QUESTION 229
An assistant from the HR Department calls you to ask the Service Hours & Maintenance Slots for your ERP system. In which document will you most probably find this information?

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

Answer: A

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

NEW QUESTION 231
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CSSLP Practice Exam Features:

* CSSLP Questions and Answers Updated Frequently

* CSSLP Practice Questions Verified by Expert Senior Certified Staff

* CSSLP Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CSSLP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year