

## CSSLP Dumps

### Certified Information Systems Security Professional

<https://www.certleader.com/CSSLP-dumps.html>



**NEW QUESTION 1**

Which of the following statements is true about residual risks?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 2**

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 3**

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 4**

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 5**

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 6**

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 7**

Which of the following is an example of over-the-air (OTA) provisioning in digital rights management?

- A. Use of shared secrets to initiate or rebuild trust.
- B. Use of software to meet the deployment goals.
- C. Use of concealment to avoid tampering attacks.
- D. Use of device properties for unique identification.

**Answer: A**

**Explanation:**

Over- the- air provisioning is a mechanism to deploy MIDlet suites over a network. It is a method of distributing MIDlet suites. MIDlet suite providers install their MIDlet suites on Web servers and provide a hypertext link for downloading. A user can use this link to download the MIDlet suite either through the Internet microbrowser or through WAP on his device. Over-the-air provisioning is required for end-to-end encryption or other security purposes in order to deliver copyrighted software to a mobile device. For example, use of shared secrets to initiate or rebuild trust. Answer D and C are incorrect. The use of device properties for unique identification and the use of concealment to avoid tampering attacks are the security challenges in digital rights management (DRM). Answer B is incorrect. The use of software and hardware to meet the deployment goals is a distracter.

**NEW QUESTION 8**

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 9**

Which of the following cryptographic system services ensures that information will not be disclosed to any unauthorized person on a local network?

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

**Answer:** D

**Explanation:**

The confidentiality service of a cryptographic system ensures that information will not be disclosed to any unauthorized person on a local network.

**NEW QUESTION 10**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 10**

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

**NEW QUESTION 13**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 17**

Which of the following organizations assists the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies?

- A. OMB
- B. NIST
- C. NSA/CSS
- D. DCAA

**Answer:** A



**Explanation:**

The Office of Management and Budget (OMB) is a Cabinet-level office, and is the largest office within the Executive Office of the President (EOP) of the United States. The current OMB Director is Peter Orszag and was appointed by President Barack Obama. The OMB's predominant mission is to assist the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies. In helping to formulate the President's spending plans, the OMB evaluates the effectiveness of agency programs, policies, and procedures, assesses competing funding demands among agencies, and sets funding priorities. The OMB ensures that agency reports, rules, testimony, and proposed legislation are consistent with the President's Budget and with Administration policies.

Answer D is incorrect. The DCAA has the aim to monitor contractor costs and perform contractor audits. Answer C is incorrect. The National Security Agency/Central Security Service (NSA/CSS) is a crypto-logic intelligence agency of the United States government. It is administered as part of the United States Department of Defense. NSA is responsible for the collection and analysis of foreign communications and foreign signals intelligence, which involves cryptanalysis. NSA is also responsible for protecting U.S. government communications and information systems from similar agencies elsewhere, which involves cryptography. NSA is a key component of the U.S. Intelligence Community, which is headed by the Director of National Intelligence. The Central Security Service is a co-located agency created to coordinate intelligence activities and co-operation between NSA and U.S. military cryptanalysis agencies. NSA's work is limited to communications intelligence. It does not perform field or human intelligence activities. Answer B is incorrect. The 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.

**NEW QUESTION 18**

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

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

**Answer:** A

**Explanation:**

John will perform OS fingerprinting on the We-are-secure network. Fingerprinting is the easiest way to detect the Operating System (OS) of a remote system. OS detection is important because, after knowing the target system's OS, it becomes easier to hack into the system. The comparison of data packets that are sent by the target system is done by fingerprinting. The analysis of data packets gives the attacker a hint as to which operating system is being used by the remote system. There are two types of fingerprinting techniques as follows: 1.Active fingerprinting 2.Passive fingerprinting In active fingerprinting ICMP messages are sent to the target system and the response message of the target system shows which OS is being used by the remote system. In passive fingerprinting the number of hops reveals the OS of the remote system. Answer D and B are incorrect. John should perform OS fingerprinting first, after which it will be easy to identify which services are running on the network since there are many services that run only on a specific operating system. After performing OS fingerprinting, John should perform networking mapping. Answer C is incorrect. This is a pre-attack phase, and only after gathering all relevant knowledge of a network should John install a backdoor.

**NEW QUESTION 23**

Which of the following roles is also known as the accreditor?

- A. Data owner
- B. Chief Risk Officer
- C. Chief Information Officer
- D. Designated Approving Authority

**Answer:** D

**Explanation:**

Designated Approving Authority (DAA) is also known as the accreditor. Answer A is incorrect. The data owner (information owner) is usually a member of management, in charge of a specific business unit, and is ultimately responsible for the protection and use of a specific subset of information. Answer B is incorrect. A Chief Risk Officer (CRO) is also known as Chief Risk Management Officer (CRMO). The Chief Risk Officer or Chief Risk Management Officer of a corporation is the executive accountable for enabling the efficient and effective governance of significant risks, and related opportunities, to a business and its various segments. Risks are commonly categorized as strategic, reputational, operational, financial, or compliance-related. CRO's are accountable to the Executive Committee and The Board for enabling the business to balance risk and reward. In more complex organizations, they are generally responsible for coordinating the organization's Enterprise Risk Management (ERM) approach. Answer C is incorrect. The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise responsible for the information technology and computer systems that support enterprise goals. The CIO plays the role of a leader and reports to the chief executive officer, chief operations officer, or chief financial officer. In military organizations, they report to the commanding officer.

**NEW QUESTION 28**

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

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

**Answer:** AC

**Explanation:**

Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The C&A process is used extensively in the U.S. Federal Government. Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3. Certification is a comprehensive assessment of the management, operational, and technical security controls in an

information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

**NEW QUESTION 32**

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 Committee	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 36**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 39**

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

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

**Answer:** A

**Explanation:**

NIST SP 800-42 provides a guideline on network security testing. Answer E, D, B, F, and C are incorrect. NIST has developed a suite of documents for conducting Certification & Accreditation (C&A). These documents are as follows: NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems. NIST Special Publication 800-53: This document provides a guideline for security controls for Federal Information Systems. NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security

controls in Federal Information System. NIST Special Publication 800-59: This document is a guideline for identifying an information system as a National Security System. NIST Special Publication 800-60: This document is a guide for mapping types of information and information systems to security objectives and risk levels.

**NEW QUESTION 42**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 46**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 47**

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

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

**Answer:** BCD

**Explanation:**

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

**NEW QUESTION 48**

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

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

**Answer:** B

**Explanation:**

The potential impact is called low if the loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational operations,



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

**NEW QUESTION 52**

Which of the following is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in business continuity?

- A. RTO
- B. RTA
- C. RPO
- D. RCO

**Answer:** A

**Explanation:**

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

**NEW QUESTION 55**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 59**

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

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

**Answer:** D

**Explanation:**

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



before performing a malicious attack. These activities are used to increase the probability of successful operation against the target, and to increase the probability of hiding the attacker's identity. Answer B is incorrect. OS fingerprinting is a process in which an external host sends special traffic on the external network interface of a computer to determine the computer's operating system. It is one of the primary steps taken by hackers in preparing an attack.

**NEW QUESTION 60**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 63**

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 68**

The Information System Security Officer (ISSO) and Information System Security Engineer (ISSE) play the role of a supporter and advisor, respectively. Which of the following statements are true about ISSO and ISSE? Each correct answer represents a complete solution. Choose all that apply.

- A. An ISSE manages the security of the information system that is slated for Certification & Accreditation (C&A).
- B. An ISSE provides advice on the continuous monitoring of the information system.
- C. An ISSO manages the security of the information system that is slated for Certification & Accreditation (C&A).
- D. An ISSE provides advice on the impacts of system change
- E. An ISSO takes part in the development activities that are required to implement system changes.

**Answer:** BCD

**Explanation:**

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. An Information System Security Engineer (ISSE) plays the role of an advisor. The responsibilities of an Information System Security Engineer are as follows: Provides view on the continuous monitoring of the information system. Provides advice on the impacts of system changes. Takes part in the configuration management process. Takes part in the development activities that are required to implement system changes. Follows approved system changes.

**NEW QUESTION 71**

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

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

**Answer:** BCD

**Explanation:**

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

**NEW QUESTION 76**

DoD 8500.2 establishes IA controls for information systems according to the Mission Assurance Categories (MAC) and confidentiality levels. Which of the following MAC levels requires high integrity and medium availability?

- A. MAC III
- B. MAC IV
- C. MAC I
- D. MAC II

**Answer:** D

**Explanation:**

The various MAC levels are as follows: MAC I: It states that the systems have high availability and high integrity. MAC II: It states that the systems have high integrity and medium availability. MAC III: It states that the systems have basic integrity and availability.

**NEW QUESTION 81**

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 82**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 86**

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

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

**Answer:** C

**Explanation:**

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

protected or sensitive data. For example:

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

**NEW QUESTION 90**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 92**

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 95**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 99**

According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Which of the following are among the eight areas of IA defined by DoD? Each correct answer represents a complete solution. Choose all that apply.

- A. VI Vulnerability and Incident Management
- B. Information systems acquisition, development, and maintenance
- C. DC Security Design & Configuration
- D. EC Enclave and Computing Environment

**Answer:** ACD

**Explanation:**

According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Following are the various U.S. Department of Defense information security standards: DC Security Design & Configuration IA Identification and Authentication EC Enclave and Computing Environment EB Enclave Boundary Defense PE Physical and Environmental PR Personnel CO Continuity VI Vulnerability and Incident Management Answer B is incorrect. Business continuity management is an International information security standard.

**NEW QUESTION 102**

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 105**

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

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

**Answer:** C

**Explanation:**

The various phases of NIST SP 800-37 C&A are as follows:

Phase 1: Initiation- This phase includes preparation, notification and resource identification. It performs the security plan analysis, update, and acceptance. Phase 2: Security Certification- The Security certification phase evaluates the controls and documentation. Phase 3: Security Accreditation- The security accreditation phase examines the residual risk for acceptability, and prepares the final security accreditation package. Phase 4: Continuous Monitoring-This phase monitors the configuration management and control, ongoing security control verification, and status reporting and documentation.

**NEW QUESTION 106**

CORRECT TEXT

Fill in the blank with an appropriate phrase. models address specifications, requirements, design, verification and validation, and maintenance activities.

- A. Life cycle

**Answer:** A

**Explanation:**

A life cycle model helps to provide an insight into the development process and emphasizes on the relationships among the different activities in this process. This model describes a structured approach to the development and adjustment process involved in producing and maintaining systems. The life cycle model addresses specifications, design, requirements, verification and validation, and maintenance activities.

**NEW QUESTION 109**

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 111**

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

- A. A-rated
- B. B-rated



- C. D-rated
- D. C-rated

**Answer: B**

**Explanation:**

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

**NEW QUESTION 114**

Which of the following individuals inspects whether the security policies, standards, guidelines, and procedures are efficiently performed in accordance with the company's stated security objectives?

- A. Information system security professional
- B. Data owner
- C. Senior management
- D. Information system auditor

**Answer: D**

**Explanation:**

An information system auditor is an individual who inspects whether the security policies, standards, guidelines, and procedures are efficiently performed in accordance with the company's stated security objectives. He is responsible for reporting the senior management about the value of security controls by performing regular and independent audits. Answer B is incorrect. A data owner determines the sensitivity or classification levels of data. Answer A is incorrect. An informational systems security professional is an individual who designs, implements, manages, and reviews the security policies, standards, guidelines, and procedures of the organization. He is responsible to implement and maintain security by the senior-level management. Answer C is incorrect. A senior management assigns overall responsibilities to other individuals.

**NEW QUESTION 115**

DRAG DROP Drag and drop the appropriate principle documents in front of their respective functions.

Principle document	Function	
Drop Here	It establishes a national risk management policy for national security systems.	CNSSP 22
Drop Here	It combines DCID 6/3, DOD Instructions 8500.2, NIST SP 800-53, and other security sources.	CNSSI 1253
Drop Here	It offers the techniques to assess adequacy of each security control.	CNSSI 1253A
Drop Here	It provides guidance to organizations with the characterization of their information and information systems.	CNSSI 1260

- 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 120**

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 123**

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

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

**Answer:** ABC

**Explanation:**

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

**NEW QUESTION 125**

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 130**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 134**

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

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

**Answer:** ACDE

**Explanation:**

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

**NEW QUESTION 139**

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 141**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 144**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 147**

The build environment of secure coding consists of some tools that actively support secure specification, design, and implementation. Which of the following features do these tools have? Each correct answer represents a complete solution. Choose all that apply.

- A. They decrease the exploitable flaws and weaknesses.
- B. They reduce and restrain the propagation, extent, and damage that have occurred by insecure software behavior.
- C. They decrease the attack surface.
- D. They employ software security constraints, protections, and service
- E. They decrease the level of type checking and program analysis.

**Answer:** ABCD

**Explanation:**

The tools that produce secure software have the following features: They decrease the exploitable flaws and weaknesses. They decrease the attack surface. They employ software security constraints, protections, and services. They reduce and restrain the propagation, extent, and damage that are caused by the behavior of insecure software. Answer E is incorrect. This feature is not required for these tools.

**NEW QUESTION 148**

Stella works as a system engineer for BlueWell Inc. She wants to identify the performance thresholds of each build. Which of the following tests will help Stella to achieve her task?

- A. Reliability test
- B. Performance test

- C. Regression test
- D. Functional test

**Answer:** B

**Explanation:**

The various types of internal tests performed on builds are as follows: Regression tests: It is also known as the verification testing. These tests are developed to confirm that capabilities in earlier builds continue to work correctly in the subsequent builds. Functional test: These tests emphasize 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 153**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 158**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 162**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 163**

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 165**

DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. What phases are identified by DIACAP? Each correct answer represents a complete solution. Choose all that apply.

- A. System Definition
- B. Validation
- C. Identification
- D. Accreditation
- E. Verification
- F. Re-Accreditation

**Answer:** ABEF

**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. DIACAP replaced the former process, known as DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process), in 2006. DoD Instruction (DoDI) 8510.01 establishes a standard DoD-wide process with a set of activities, general tasks, and a management structure to certify and accredit an Automated Information System (AIS) that will maintain the Information Assurance (IA) posture of the Defense Information Infrastructure (DII) throughout the system's life cycle. DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. It identifies four phases: \* 1.System Definition 2.Verification 3.Validation 4.Re-Accreditation

**NEW QUESTION 167**

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

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

**Answer:** ABCD

**Explanation:**

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

- \* 1.Configuration identification: Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined.
- \* 2.Configuration change control: Configuration change control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them.
- \* 3.Configuration status accounting: Configuration status accounting is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time.
- \* 4.Configuration audits: Configuration audits are broken into functional and physical configuration audits. They occur either at delivery or at the moment of effecting the change. A functional configuration audit ensures that functional and performance attributes of a configuration item are achieved, while a physical configuration audit ensures that a configuration item is installed in accordance with the requirements of its detailed design documentation.

**NEW QUESTION 170**

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

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

**Answer:** B

**Explanation:**

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

businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption. Answer D is incorrect. A disaster recovery plan should contain data, hardware, and software that can be critical for a business. It should also include the plan for sudden loss such as hard disc crash. The business should use backup and data recovery utilities to limit the loss of data.

**NEW QUESTION 172**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 173**

Which of the following types of attacks is targeting a Web server with multiple compromised computers that are simultaneously sending hundreds of FIN packets with spoofed IP source IP addresses?

- A. DDoS attack
- B. Evasion attack
- C. Insertion attack
- D. Dictionary attack

**Answer:** A

**Explanation:**

A distributed denial of service (DDoS) attack targets a Web server with multiple compromised computers that are simultaneously sending hundreds of FIN packets with spoofed IP source IP addresses. DDoS attack occurs when multiple compromised systems flood the bandwidth or resources of a targeted system, usually one or more Web servers. These systems are compromised by attackers using a variety of methods. It is an attempt to make a computer resource unavailable to its intended users. This type of attack can cause the following to occur: Saturate network resources. Disrupt connections between two computers, thereby preventing communications between services. Disrupt services on a specific computer. Answer D is incorrect. Dictionary attack is a type of password guessing attack. This type of attack uses a dictionary of common words to find out the password of a user. It can also use common words in either upper or lower case to find a password. There are many programs available on the Internet to automate and execute dictionary attacks. Answer C is incorrect. In an insertion attack, an IDS accepts a packet and assumes that the host computer will also accept it. But in reality, when a host system rejects the packet, the IDS accepts the attacking string that will exploit vulnerabilities in the IDS. Such attacks can badly infect IDS signatures and IDS signature analysis. Answer B is incorrect. An evasion attack is one in which an IDS rejects a malicious packet but the host computer accepts it. Since an IDS has rejected it, it does not check the contents of the packet. Hence, using this technique, an attacker can exploit the host computer. In many cases, it is quite simple for an attacker to send such data packets that can easily perform evasion attacks on an IDSs.

**NEW QUESTION 178**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 180**

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

test the software?

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

**Answer: B**

**Explanation:**

Regression testing can be performed any time when a program needs to be modified either to add a feature or to fix an error. It is a process of repeating Unit testing and Integration testing whenever existing tests need to be performed again along with the new tests. Regression testing is performed to ensure that no existing errors reappear, and no new errors are introduced. Answer D is incorrect. The acceptance testing is performed on the application before its implementation into the production environment. It is done either by a client or an application specialist to ensure that the software meets the requirement for which it was made. Answer A is incorrect. Integration testing is a logical extension of unit testing. It is performed to identify the problems that occur when two or more units are combined into a component. During integration testing, a developer combines two units that have already been tested into a component, and tests the interface between the two units. Although integration testing can be performed in various ways, the following three approaches are generally used: The top-down approach The bottom-up approach The umbrella approach Answer B is incorrect. Unit testing is a type of testing in which each independent unit of an application is tested separately. During unit testing, a developer takes the smallest unit of an application, isolates it from the rest of the application code, and tests it to determine whether it works as expected. Unit testing is performed before integrating these independent units into modules. The most common approach to unit testing requires drivers and stubs to be written. Drivers and stubs are programs. A driver simulates a calling unit, and a stub simulates a called unit.

**NEW QUESTION 183**

Which of the following security models dictates that subjects can only access objects through applications?

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 187**

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

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

**Answer: ABD**

**Explanation:**

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

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

**NEW QUESTION 192**

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

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

**Answer: D**

**Explanation:**

This is an example of transference. When the risk is transferred to a third party, usually for a fee, it creates a contractual-relationship for the third party to manage the risk on behalf of the performing organization. Risk response planning is a method of developing options to decrease the amount of threats and make the most of opportunities. The risk response should be aligned with the consequence of the risk and cost- effectiveness. This planning documents the processes for managing risk events. It addresses the owners and their responsibilities, risk identification, results from qualification and quantification processes, budgets and times for responses, and contingency plans. The various risk response planning techniques are as follows: Risk acceptance: It indicates that the project team has decided not to change the project management plan to deal with a risk, or is unable to identify any other suitable response strategy. Risk avoidance: It is a

technique for a threat, which creates changes to the project management plan that are meant to either eliminate the risk or to protect the project objectives from this impact. Risk mitigation: It is a list of specific actions being taken to deal with specific risks associated with the threats and seeks to reduce the probability of occurrence or impact of risk below an acceptable threshold. Risk transference: It is used to shift the impact of a threat to a third party, together with the ownership of the response.

**NEW QUESTION 196**

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 197**

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

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

**Answer:** A

**Explanation:**

Anonymous authentication is an authentication method used for Internet communication. It provides limited access to specific public folders and directory information or public areas of a Web site. It is supported by all clients and is used to access unsecured content in public folders. An administrator must create a user account in IIS to enable the user to connect anonymously. Answer D is incorrect. Multi-factor authentication involves a combination of multiple methods of authentication. For example, an authentication method that uses smart cards as well as usernames and passwords can be referred to as multi-factor authentication. Answer 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 B 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 199**

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 204**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 207**

Which of the following are the primary functions of configuration management? Each correct answer represents a complete solution. Choose all that apply.

- A. It removes the risk event entirely by adding additional steps to avoid the event.
- B. It ensures that the change is implemented in a sequential manner through formalized testing.
- C. It reduces the negative impact that the change might have had on the computing services and resources.
- D. It analyzes the effect of the change that is implemented on the system.



**Answer:** BCD

**Explanation:**

The primary functions of configuration management are as follows: It ensures that the change is implemented in a sequential manner through formalized testing. It ensures that the user base is informed of the future change. It analyzes the effect of the change that is implemented on the system. It reduces the negative impact that the change might have had on the computing services and resources. Answer A is incorrect. It is not one of the primary functions of configuration management. It is the function of risk avoidance.

**NEW QUESTION 212**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 213**

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 214**

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 216**

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

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

**Answer:** D

**Explanation:**

In order to accomplish the task, you should use the software testing technique. By using this technique you can determine compatibility of systems with custom applications or you can identify other unforeseen interactions. You can also use the software testing technique while you are upgrading software. Answer B is

incorrect. You can use the antivirus management to save the systems from viruses, unexpected software interactions, and the subversion of security controls. Answer A is incorrect. You can use the safe software storage technique to ensure that the software and backup copies have not been modified without authorization. Answer B is incorrect. You can use the backup control to perform back up of software and data.

**NEW QUESTION 218**

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 219**

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

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

**Answer:** AD

**Explanation:**

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

**NEW QUESTION 222**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 225**

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

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

**Answer:** BCDE

**Explanation:**

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

**NEW QUESTION 230**

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 235**

Which of the following phases of the DITSCAP C&A process is used to define the C&A level of effort, to identify the main C&A roles and responsibilities, and to create an agreement on the method for implementing the security requirements?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 237**

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 240**

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 243**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 245**

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 247**

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 249**

Companies use some special marks to distinguish their products from those of other companies. These marks can include words, letters, numbers, drawings, etc. Which of the following terms describes these special marks?

- A. Business mark
- B. Trademark
- C. Sales mark
- D. Product mark

**Answer: B**

**Explanation:**

A trademark is a mark that is used by a company to distinguish its products from those of other companies. There are various ways a company uses its trademark to distinguish its products from others. It can use words, letters, numbers, drawings, pictures, and so on, in its trademark. Answer D, A, and C are incorrect. There is no such mark as product mark, business mark, or sales mark.

**NEW QUESTION 253**

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

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

**Answer: B**

**Explanation:**

The Annualized Rate of Occurrence (ARO) is a number that represents the estimated frequency at which a threat is expected to occur. It is calculated based upon the probability of the event occurring and the number of employees that could make that event occur. Answer D is incorrect. The Exposure Factor (EF) represents the % of assets loss caused by a threat. The EF is required to calculate the Single Loss Expectancy (SLE).

Answer A is incorrect. The Single Loss Expectancy (SLE) is the value in dollars that is assigned to a single event.  $SLE = \text{Asset Value (\$)} \times \text{Exposure Factor (EF)}$

Answer B is incorrect. Safeguard acts as a countermeasure for reducing the risk associated with a specific threat or a group of threats.

**NEW QUESTION 254**

.....



## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your CSSLP Exam with Our Prep Materials Via below:**

<https://www.certleader.com/CSSLP-dumps.html>