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

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

Risk Adjustments: Contingency plans and exceptions should be generated so that the residual risk be above the acceptable threshold.

QUESTION 138
Which of the following provides an easy way to programmers for writing lower-risk applications and retrofitting security into an existing application?

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

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

QUESTION 139
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.

QUESTION 140
An attacker exploits actual code of an application and uses a security hole to carry out an attack before the application vendor knows about the vulnerability. Which of the following types of attack is this?

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

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

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

QUESTION 141
You are the project manager for your organization. You are preparing for the quantitative risk analysis. Mark, a project team member, wants to know why you need to do quantitative risk analysis when you just completed qualitative risk analysis. Which one of the following statements best defines what quantitative risk analysis is?

A. Quantitative risk analysis is the process of prioritizing risks for further analysis or action by assessing and combining their probability of occurrence and impact.
B. Quantitative risk analysis is the review of the risk events with the high probability and the highest impact on the project objectives.
C. Quantitative risk analysis is the planning and quantification of risk responses based on probability and impact of each risk event.
D. Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives.

Answer: D
Explanation:
Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives. It is performed on risk that have been prioritized through the qualitative risk analysis process. Answer: A is incorrect. This is actually the definition of qualitative risk analysis. Answer: B is incorrect. While somewhat true, this statement does not completely define the quantitative risk analysis process. Answer: C is incorrect. This is not a valid statement about the quantitative risk analysis process. Risk response planning is a separate project management process.

QUESTION 142
You work as a security engineer for BlueWell Inc. According to you, which of the following DITSCAP/NIACAP model phases occurs at the initiation of the project, or at the initial C&A effort of a legacy system?

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

Answer: B
Explanation:
The definition phase of the DITSCAP/NIACAP model takes place at the beginning of the project, or at the initial C&A effort of a legacy system. C&A consists of four phases in a DITSCAP assessment. These phases are the same as NIACAP phases. The order of these phases is as follows: 1.Definition: The definition phase is focused on understanding the IS business case, the mission, environment, and architecture. This phase determines the security requirements and level of effort necessary to achieve Certification & Accreditation (C&A). 2.Verification: The second phase confirms the evolving or modified system's compliance with the information. The verification phase ensures that the fully integrated system will be ready for certification testing. 3.Validation: The third phase confirms abidance of the fully integrated system with the security

policy. This phase follows the requirements slated in the SSAA. The objective of the validation phase is to show the required evidence to support the DAA in accreditation process. 4.Post Accreditation: The Post Accreditation is the final phase of DITSCAP assessment and it starts after the system has been certified and accredited for operations. This phase ensures secure system management, operation, and maintenance to save an acceptable level of residual risk.

QUESTION 143
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.

QUESTION 144
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 services.
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.

QUESTION 145
Which of the following requires all general support systems and major applications to be fully certified and accredited before these systems and applications are put into production? Each

correct answer represents a part of the solution. Choose all that apply.

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

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

QUESTION 146
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.

QUESTION 147
Which of the following persons in an organization is responsible for rejecting or accepting the residual risk for a system?