QUESTION 30
You work as a systems engineer for BlueWell Inc. Which of the following tools will you use to look outside your own organization to examine how others achieve their performance levels, and what processes they use to reach those levels?

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

Answer: A

QUESTION 31
Which of the following methods determines the principle name of the current user and returns the jav a.security.Principal object in the HttpServletRequest interface?

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

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

QUESTION 32
The NIST Information Security and Privacy Advisory Board (ISPAB) paper "Perspectives on Cloud Computing and Standards" specifies potential advantages and disdvantages of virtualization. Which of the following disadvantages does it include? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: CDEFG
Explanation:
The potential security disadvantages of virtualization are as follows: It increases configuration effort because of complexity and composite system. It initiates the problem of how to prevent

overlap while mapping VM storage onto host files. It introduces the problem of virtualizing the TPM. It creates the possibility that remote attestation may not work. It initiates the problem of detecting VM covert channels. It involves new protection mechanisms for preventing VM escape, VM detection, and VM-VM interference. It initiates the possibility of virtual networking configuration errors. It initiates the risk that malicious software is targeting the VM environment.

It increases overall security risk shared resources, such as networks, clipboards, clocks, printers, desktop management, and folders. Answer: A and B are incorrect. These are not the disadvantages of virtualization, as described in the NIST Information Security and Privacy Advisory Board (ISPAB) paper "Perspectives on Cloud Computing and Standards".

QUESTION 33
Which of the following are the types of access controls? Each correct answer represents a complete solution. Choose three.

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

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

QUESTION 34
What are the subordinate tasks of the Initiate and Plan IA C&A phase of the DIACAP process? Each correct answer represents a complete solution. Choose all that apply.

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

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

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

QUESTION 35
Which of the following attacks causes software to fail and prevents the intended users from

accessing software?

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

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

QUESTION 36
FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls have been implemented?

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

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

QUESTION 37
Which of the following is a name, symbol, or slogan with which a product is identified?

A. Trademark
B. Copyright
C. Trade secret
D. Patent
Answer: A
Explanation:
A trademark is a name, symbol, or slogan with which a product is identified. Its uniqueness makes the product noticeable among the same type of products. For example, Pentium and Athlon are brand names of the CPUs that are manufactured by Intel and AMD, respectively. The trademark law protects a company's trademark by making it illegal for other companies to use it without taking prior permission of the trademark owner. A trademark is registered so that others cannot use identical or similar marks. Answer: C is incorrect. A trade secret is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known. It

helps a business to obtain an economic advantage over its competitors or customers. In some jurisdictions, such secrets are referred to as confidential information or classified information. Answer: B is incorrect. A copyright is a form of intellectual property, which secures to its holder the exclusive right to produce copies of his or her works of original expression, such as a literary work, movie, musical work or sound recording, painting, photograph, computer program, or industrial design, for a defined, yet extendable, period of time. It does not cover ideas or facts. Copyright laws protect intellectual property from misuse by other individuals. Answer: D is incorrect. A patent is a set of exclusive rights granted to anyone who invents any new and useful machine, process, composition of matter, etc. A patent enables the inventor to legally enforce his right to exclude others from using his invention.

QUESTION 38
Della work as a project manager for BlueWell Inc. A threat with a dollar value of $250,000 is expected to happen in her project and the frequency of threat occurrence per year is 0.01. What will be the annualized loss expectancy in her project?

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

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

ALE = SLE * ARO

= 250,000 * 0.01

= 2,500

Answer: D, C, and A are incorrect. These are not valid answers.

QUESTION 39
Which of the following coding practices are helpful in simplifying code? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABC
Explanation:
The various coding practices that are helpful in simplifying the code are as follows: Programmers should implement high-consequence functions in minimum required lines of code and follow the proper coding standards. Software should implement the functions that are defined in the

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

QUESTION 40
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.

QUESTION 41
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.

QUESTION 42