D. Risk assessment and treatment

Answer: BCD
Explanation:
Following are the various international information security standards:

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

QUESTION 127
The Data and Analysis Center for Software (DACS) specifies three general principles for software assurance which work as a framework in order to categorize various secure design principles. Which of the following principles and practices does the General Principle 1 include? Each correct answer represents a complete solution. Choose two.

A. Principle of separation of privileges, duties, and roles
B. Assume environment data is not trustworthy
C. Simplify the design
D. Principle of least privilege

Answer: AD
Explanation:
General Principle 1- Minimize the number of high-consequence targets includes the following principles and practices:

Principle of least privilege Principle of separation of privileges, duties, and roles Principle of separation of domains Answer: B is incorrect. Assume environment data is not trustworthy principle is included in the General Principle 2. Answer: C is incorrect. Simplify the design principle is included in the General Principle 3.

QUESTION 128
CORRECT TEXT
Fill in the blank with the appropriate security mechanism. is a computer hardware mechanism or programming language construct which handles the occurrence of exceptional events.

Answer: Exception handling

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

QUESTION 129
In which of the following phases of the DITSCAP process does Security Test and Evaluation (ST&E) occur?

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

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

QUESTION 130
Which of the following access control models uses a predefined set of access privileges for an object of a system?

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

Answer: D
Explanation:
Mandatory Access Control (MAC) is a model that uses a predefined set of access privileges for an object of the system. Access to an object is restricted on the basis of the sensitivity of the object and granted through authorization. Sensitivity of an object is defined by the label assigned to it. For example, if a user receives a copy of an object that is marked as "secret", he cannot grant permission to other users to see this object unless they have the appropriate permission. Answer: B is incorrect. DAC is an access control model. In this model, the data owner has the right to decide who can access the data. Answer: A is incorrect. Role-based access control (RBAC) is an access control model. In this model, a user can access resources according to his

role in the organization. For example, a backup administrator is responsible for taking backups of important data. Therefore, he is only authorized to access this data for backing it up. However, sometimes users with different roles need to access the same resources. This situation can also be handled using the RBAC model. Answer: C is incorrect. There is no such access control model as Policy Access Control.

QUESTION 131

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: C is incorrect. Unit testing is a type of testing in which each independent unit of an application is tested separately. During unit testing, a developer takes the smallest unit of an application, isolates it from the rest of the application code, and tests it to determine whether it works as expected. Unit testing is performed before integrating these independent units into modules. The most common approach to unit testing requires drivers and stubs to be written. Drivers and stubs are programs. A driver simulates a calling unit, and a stub simulates a called unit.

QUESTION 132

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

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

Answer: ABD
Explanation:
ISO/IEC 27002 is an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC) as ISO/IEC 17799:2005. This standard contains the following twelve main sections: 1.Risk assessment: It refers to assessment of risk. 2.Security policy: It deals with the security management.

3.Organization of information security: It deals with governance of information security. 4.Asset management: It refers to inventory and classification of information assets. 5.Human resources security: It deals with security aspects for employees joining, moving and leaving an organization. 6.Physical and environmental security: It is related to protection of the computer facilities. 7.Communications and operations management: It is the management of technical security controls in systems and networks. 8.Access control: It deals with the restriction of access rights to networks, systems, applications, functions and data. 9.Information systems acquisition, development and maintenance: It refers to build security into applications. 10.Information security incident management: It refers to anticipate and respond appropriately to information security breaches. 11.Business continuity management: It deals with protecting, maintaining and recovering business-critical processes and systems.

12.Compliance: It is used for ensuring conformance with information security policies, standards, laws and regulations. Answer: C is incorrect. Financial assessment does not come under the ISO/IEC 27002 standard.

QUESTION 133

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: C is incorrect. The concept of accountability determines the actions and behaviors of a single individual within a system, and identifies that particular individual.

QUESTION 134

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: C is incorrect. This answer would only be correct if the project has a status meeting just once per month in the project. Answer: B is incorrect. Risk management happens throughout the project as does project planning.

QUESTION 135
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.

QUESTION 136
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&A. Answer: C is incorrect. Phase 2 is used to implement and validate assigned IA controls. Answer: E is incorrect. Phase 3 is used to make certification determination and accreditation decisions. Answer: B is incorrect. Phase 5 is known as decommission system and is used to conduct activities related to the disposition of the system data and objects.

QUESTION 137
Which of the following security controls will you use for the deployment phase of the SDLC to build secure software? Each correct answer represents a complete solution. Choose all that apply.

A. Change and Configuration Control