DoD 7950.1-M: This DoD directive refers to the 'Defense Automation Resources Management Manual'. DoDD 8000.1: This DoD directive refers to the 'Defense Information Management (IM) Program'. DoD 8910.1: This DoD directive refers to the 'Management and Control of Information Requirements'.

QUESTION 75
Which of the following access control models are used in the commercial sector? Each correct answer represents a complete solution. Choose two.

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

Answer: AC
Explanation:
The Biba and Clark-Wilson access control models are used in the commercial sector. The Biba model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject. The Clark-Wilson security model provides a foundation for specifying and analyzing an integrity policy for a computing system. Answer: D is incorrect. The Bell-LaPadula access control model is mainly used in military systems. Answer: B is incorrect. There is no such access control model as Clark-Biba.

QUESTION 76
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.

QUESTION 77
Which of the following statements best describes the difference between the role of a data owner and the role of a data custodian?

A. The custodian makes the initial information classification assignments, and the operations manager implements the scheme.
B. The data owner implements the information classification scheme after the initial assignment by the custodian.
C. The custodian implements the information classification scheme after the initial assignment by the operations manager.
D. The data custodian implements the information classification scheme after the initial assignment by the data owner.

Answer: D
Explanation:
The data owner is responsible for ensuring that the appropriate security controls are in place, for assigning the initial classification to the data to be protected, for approving access requests from other parts of the organization, and for periodically reviewing the data classifications and access rights. Data owners are primarily responsible for determining the data's sensitivity or classification levels, whereas the data custodian has the responsibility for backup, retention, and recovery of data. The data owner delegates these responsibilities to the custodian. Answer: B, A, and C are incorrect. These are not the valid answers.

QUESTION 78
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.

QUESTION 79
Which of the following secure coding principles and practices defines the appearance of code listing so that a code reviewer and maintainer who have not written that code can easily understand it?

A. Make code forward and backward traceable
B. Review code during and after coding
C. Use a consistent coding style
D. Keep code simple and small

Answer: C
Explanation:
Use a consistent coding style is one of the principles and practices that contribute to defensive coding. This principle defines the appearance of code listing so that a code reviewer and maintainer who have not written that code can easily understand it. For this purpose, all programmers of a team must follow the same guidelines. Answer: D is incorrect. Keep code simple and small defines that it is easy to verify the software security when a programmer uses small and simple code base. Answer: A is incorrect. Make code forward and backward traceable defines that traceability is necessary in order to validate requirements, prevent defects, and find and solve inconsistencies among all objects generated in the SDLC phases. Answer: B is incorrect. Review code during and after coding defines that code must be examined in order to identify coding errors in modules.

QUESTION 80
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.

QUESTION 81
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

QUESTION 82
In which of the following alternative processing sites is the backup facility maintained in a constant order, with a full complement of servers, workstations, and communication links ready to assume the primary operations responsibility?

A. Cold Site
B. Hot Site
C. Warm Site
D. Mobile Site

Answer: B
Explanation:
A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data. It provides the backup facility, which is maintained in a constant order, with a full complement of servers, workstations, and communication links ready to assume the primary operations responsibility.

A hot site is a backup site in case disaster has taken place in a data center. A hot site is located off site and provides the best protection. It is an exact replica of the current data center. In case a disaster struck to the data center, administrators just need to take the backup of recent data in hot site and the data center is back online in a very short time. It is very expensive to create and maintain the hot site. There are lots of third party companies that provide disaster recovery solutions by maintaining hot sites at their end. Answer: A is incorrect. A cold site is a backup site in case disaster has taken place in a data center. This is the least expensive disaster recovery solution, usually having only a single room with no equipment. All equipment is brought to the site after the disaster. It can be on site or off site. Answer: D is incorrect. Mobile sites are self-reliant, portable shells custom-fitted with definite telecommunications and IT equipment essential to meet system requirements. These are presented for lease through commercial vendors. Answer: C is incorrect. A warm site is, quite logically, a compromise between hot and cold sites. Warm sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. These sites will have backups on hand, but they may not be complete and may be between several days and a week old. An example would be backup tapes sent to the warm site by courier.

QUESTION 83
Which of the following methods offers a number of modeling practices and disciplines that contribute to a successful service-oriented life cycle management and modeling?

A. Service-oriented modeling framework (SOMF)
B. Service-oriented architecture (SOA)
C. Sherwood Applied Business Security Architecture (SABSA)
D. Service-oriented modeling and architecture (SOMA)

Answer: A
Explanation:
The service-oriented modeling framework (SOMF) has been proposed by author Michael Bell as a service-oriented modeling language for software development that employs disciplines and a holistic language to provide strategic solutions to enterprise problems. The service-oriented modeling framework (SOMF) is a service-oriented development life cycle methodology. It offers a number of modeling practices and disciplines that contribute to a successful service-oriented life cycle management and modeling. The service-oriented modeling framework illustrates the major elements that identify the "what to do" aspects of a service development scheme. Answer: B is incorrect. The service-oriented architecture (SOA) is a flexible set of design principles used during the phases of systems development and integration. Answer: D is incorrect. The service-oriented modeling and architecture (SOMA) includes an analysis and design method that extends traditional object-oriented and component-based analysis and design methods to include concerns relevant to and supporting SOA. Answer: C is incorrect. SABSA (Sherwood Applied Business Security Architecture) is a framework and methodology for Enterprise Security Architecture and Service Management. It is a model and a methodology for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives.

QUESTION 84
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.

QUESTION 85
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