Maria has been recently appointed as a Network Administrator in Gentech Inc. She has been tasked to perform network security testing to find out the vulnerabilities and shortcomings of the present network infrastructure. Which of the following testing approaches will she apply to accomplish this task?

A. Gray-box testing
B. White-box testing
C. Black-box testing
D. Unit testing

Answer: C
Explanation:
Maria is new for this organization and she does not have any idea regarding the present infrastructure. Therefore, black box testing is best suited for her. Blackbox testing is a technique in which the testing team has no knowledge about the infrastructure of the organization. The testers must first determine the location and extent of the systems before commencing their analysis. This testing technique is costly and time consuming. Answer: B is incorrect. White box testing, also known as Clear box or Glass box testing, takes into account the internal mechanism of a system or application. The connotations of "Clear box" and "Glass box" indicate that a tester has full visibility of the internal workings of the system. It uses knowledge of the internal structure of an application. It is applicable at the unit, integration, and system levels of the software testing process. It consists of the following testing methods: Control flow-based testing Create a graph from source code. Describe the flow of control through the control flow graph. Design test cases to cover certain elements of the graph. Data flow-based testing Test connections between variable definitions. Check variation of the control flow graph. Set DEF (n) contains variables that are defined at node n. Set USE (n) are variables that are read. Answer: A is incorrect. Graybox testing is a combination of whitebox testing and blackbox testing. In graybox testing, the test engineer is equipped with the knowledge of system and designs test cases or test data based on system knowledge. The security tester typically performs graybox testing to find vulnerabilities in software and network system. Answer: D 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 195
Which of the following processes identifies the threats that can impact the business continuity of operations?

A. Function analysis
B. Risk analysis
C. Business impact analysis
D. Requirement analysis

Answer: C
Explanation:
A business impact analysis (BIA) is a crisis management and business impact analysis technique that identifies those threats that can impact the business continuity of operations. Such threats can be either natural or man-made. The BIA team should have a clear understanding of the organization, key business processes, and IT resources for assessing the risks associated with continuity. In the BIA team, there should be senior management, IT personnel, and end users to identify all resources that are to be used during normal operations. Answer: B is incorrect. Risk

analysis is the science of risks and their probability and evaluation in a business or a process. It is an important factor in security enhancement and prevention in a system. Risk analysis should be performed as part of the risk management process for each project. The outcome of the risk analysis would be the creation or review of the risk register to identify and quantify risk elements to the project and their potential impact. Answer: A is incorrect. The functional analysis process is used for converting system requirements into a comprehensive function standard. Verification is the result of the functional analysis process, in which the fundamentals of a system level functional architecture are defined adequately to allow for synthesis in the design phase. The functional analysis breaks down the higher-level functions into the lower level functions. Answer: D is incorrect. Requirements analysis encompasses the tasks that go into determining the needs or conditions to meet for a new or altered product, taking account of the possibly conflicting requirements of the various stakeholders.

QUESTION 196
The Phase 3 of DITSCAP C&A is known as Validation. The goal of Phase 3 is to validate that the preceding work has produced an IS that operates in a specified computing environment. What are the process activities of this phase? Each correct answer represents a complete solution. Choose all that apply.

A. Certification and accreditation decision
B. Continue to review and refine the SSAA
C. Perform certification evaluation of the integrated system
D. System development
E. Develop recommendation to the DAA

Answer: ABCE
Explanation:
The Phase 3 of DITSCAP C&A is known as Validation. The goal of Phase 3 is to validate that the preceding work has produced an IS that operates in a specified computing environment. The process activities of this phase are as follows: Continue to review and refine the SSAA Perform certification evaluation of the integrated system Develop recommendation to the DAA Certification and accreditation decision Answer: D is incorrect. System development is a Phase 2 activity.

QUESTION 197
Which of the following methods 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?

A. Configuration control
B. Documentation control
C. Configuration identification
D. Configuration auditing

Answer: B
Explanation:
Documentation control is a method of ensuring that system changes should be agreed upon before being implemented, only the proposed and approved changes are implemented, and the implementation is complete and accurate. Documentation control is involved in the strict events for proposing, monitoring, and approving system changes and their implementation. It helps the change process by supporting the person who synchronizes the analytical task, approves system changes, reviews the implementation of changes, and oversees other tasks such as documenting the controls. Answer: D 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. Answer: A 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. Answer: C is incorrect. 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.

QUESTION 198
Information Security management is a process of defining the security controls in order to protect information assets. The first action of a management program to implement information security is to have a security program in place. What are the objectives of a security program? Each correct answer represents a complete solution. Choose all that apply.

A. Security education
B. Security organization
C. System classification
D. Information classification

Answer: ABD
Explanation:
The first action of a management program to implement information security is to have a security program in place. The objectives of a security program are as follows: Protect the company and its assets Manage risks by identifying assets, discovering threats, and estimating the risk Provide direction for security activities by framing of information security policies, procedures, standards, guidelines and baselines Information classification Security organization Security education Answer: C is incorrect. System classification is not one of the objectives of a security program.

QUESTION 199
What NIACAP certification levels are recommended by the certifier? Each correct answer represents a complete solution. Choose all that apply.

A. Comprehensive Analysis
B. Maximum Analysis
C. Detailed Analysis
D. Minimum Analysis
E. Basic Security Review
F. Basic System Review

Answer: ACDE
Explanation:
NIACAP has four levels of certification. These levels ensure that the appropriate C&A are performed for varying schedule and budget limitations. The certifier must analyze the system's business functions. The certifier determines the degree of confidentiality, integrity, availability,

and accountability, and then recommends one of the following NIACAP certification levels: Level 1 - Basic Security Review Level 2 - Minimum Analysis Level 3 - Detailed Analysis Level 4 - Comprehensive Analysis Answer: B and F are incorrect. No such types of levels exist.

QUESTION 200
Which of the following intrusion detection systems (IDS) monitors network traffic and compares it against an established baseline?

A. File-based
B. Network-based
C. Anomaly-based
D. Signature-based

Answer: C
Explanation:
The anomaly-based intrusion detection system (IDS) monitors network traffic and compares it against an established baseline. This type of IDS monitors traffic and system activity for unusual behavior based on statistics. In order to identify a malicious activity, it learns normal behavior from the baseline. The anomaly-based intrusion detection is also known as behavior-based or statistical-based intrusion detection. Answer: D is incorrect. Signature-based IDS uses a database with signatures to identify possible attacks and malicious activity. Answer: B is incorrect. A network-based IDS can be a dedicated hardware appliance, or an application running on a computer, attached to the network. It monitors all traffic in a network or traffic coming through an entry-point such as an Internet connection. Answer: A is incorrect. There is no such intrusion detection system (IDS) that is file-based.

QUESTION 201
Which of the following characteristics are described by the DIAP Information Readiness Assessment function? Each correct answer represents a complete solution. Choose all that apply.

A. It provides for entry and storage of individual system data.
B. It performs vulnerability/threat analysis assessment.
C. It provides data needed to accurately assess IA readiness.
D. It identifies and generates IA requirements.

Answer: BCD
Explanation:
The characteristics of the DIAP Information Readiness Assessment function are as follows: It provides data needed to accurately assess IA readiness. It identifies and generates IA requirements. It performs vulnerability/threat analysis assessment. Answer: A is incorrect. It is a function performed by the ASSET system.

QUESTION 202
Which of the following classification levels defines the information that, if disclosed to the unauthorized parties, could be reasonably expected to cause exceptionally grave damage to the national security?

A. Secret information
B. Unclassified information
C. Confidential information
D. Top Secret information

Answer: D
Explanation:
Top Secret information is the highest level of classification of material on a national level. Such material would cause "exceptionally grave damage" to national security if publicly available. Answer: A is incorrect. Secret information is that, if disclosed to unauthorized parties, could be expected to cause serious damage to the national security, but it is not the best answer for the above question. Answer: C is incorrect. Such material would cause "damage" or be "prejudicial" to national security if publicly available. Answer: B is incorrect. Unclassified information, technically, is not a classification level, but is used for government documents that do not have a classification listed above. Such documents can sometimes be viewed by those without security clearance.

QUESTION 203
Which of the following security design principles supports comprehensive and simple design and implementation of protection mechanisms, so that an unintended access path does not exist or can be readily identified and eliminated?

A. Least privilege
B. Economy of mechanism
C. Psychological acceptability
D. Separation of duties

Answer: B
Explanation:
The economy of mechanism is a security design principle, which supports simple and comprehensive design and implementation of protection mechanisms, so that an unintended access path does not exist or can be readily identified and eliminated. Answer: D is incorrect. Separation of duties defines that the completion of a specific sensitivity activity or access to sensitive object depends on the satisfaction of multiple conditions. Answer: C is incorrect. Psychological acceptability defines the ease of use and intuitiveness of the user interface that controls and interacts with the access control mechanisms. Answer: A is incorrect. Least privilege maintains that an individual, process, or other type of entity should be given the minimum privileges and resources for the minimum period of time required to complete a task.

QUESTION 204
Rob is the project manager of the IDLK Project for his company. This project has a budget of $5,600,000 and is expected to last 18 months. Rob has learned that a new law may affect how the project is allowed to proceed - even though the organization has already invested over $750,000 in the project. What risk response is the most appropriate for this instance?

A. Transference
B. Enhance
C. Mitigation
D. Acceptance

Answer: D
Explanation:
At this point all that Rob can likely do is accepting the risk event. Because this is an external risk, there is little that Rob can do other than document the risk and share the new with management and the project stakeholders. If the law is passed then Rob can choose the most appropriate way for the project to continue. Acceptance response is a part of Risk Response planning process. Acceptance response delineates that the project plan will not be changed to deal with the risk.