of effect and theoretical response. The inputs to the Qualitative Risk Analysis process are: Organizational process assets Project Scope Statement Risk Management Plan Risk Register Answer: B is incorrect. Historical information can be helpful in the qualitative risk analysis, but it is not the best answer for the question as historical information is not always available (consider new projects). Answer: D is incorrect. Quantitative risk analysis is in-depth and often requires a schedule and budget for the analysis. Answer: C is incorrect. Rolling wave planning is not a valid answer for risk analysis processes.

QUESTION 10
Which of the following models uses a directed graph to specify the rights that a subject can transfer to an object or that a subject can take from another subject?

A. Take-Grant Protection Model
B. Biba Integrity Model
C. Bell-LaPadula Model
D. Access Matrix

Answer: A
Explanation:
The take-grant protection model is a formal model used in the field of computer security to establish or disprove the safety of a given computer system that follows specific rules. It shows that for specific systems the question of safety is decidable in linear time, which is in general undecidable. The model represents a system as directed graph, where vertices are either subjects or objects. The edges between them are labeled and the label indicates the rights that the source of the edge has over the destination. Two rights occur in every instance of the model: take and grant. They play a special role in the graph rewriting rules describing admissible changes of the graph. Answer: D is incorrect. The access matrix is a straightforward approach that provides access rights to subjects for objects. Answer: C is incorrect. The Bell-LaPadula model deals only with the confidentiality of classified material. It does not address integrity or availability. Answer: B is incorrect. The integrity model was developed as an analog to the Bell-LaPadula confidentiality model and then became more sophisticated to address additional integrity requirements.

QUESTION 11
You are the project manager for GHY Project and are working to create a risk response for a negative risk. You and the project team have identified the risk that the project may not complete on time, as required by the management, due to the creation of the user guide for the software you're creating. You have elected to hire an external writer in order to satisfy the requirements and to alleviate the risk event. What type of risk response have you elected to use in this instance?

A. Transference
B. Exploiting
C. Avoidance
D. Sharing

Answer: A
Explanation:
This is an example of transference as you have transferred the risk to a third party. Transference almost always is done with a negative risk event and it usually requires a contractual relationship.
QUESTION 12
Which of the following organizations assists the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies?

A. OMB
B. NIST
C. NSA/CSS
D. DCAA

Answer: A
Explanation:
The Office of Management and Budget (OMB) is a Cabinet-level office, and is the largest office within the Executive Office of the President (EOP) of the United States. The current OMB Director is Peter Orszag and was appointed by President Barack Obama. The OMB's predominant mission is to assist the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies. In helping to formulate the President's spending plans, the OMB evaluates the effectiveness of agency programs, policies, and procedures, assesses competing funding demands among agencies, and sets funding priorities. The OMB ensures that agency reports, rules, testimony, and proposed legislation are consistent with the President's Budget and with Administration policies.

Answer: D is incorrect. The DCAA has the aim to monitor contractor costs and perform contractor audits. Answer: C is incorrect. The National Security Agency/Central Security Service (NSA/CSS) is a crypto-logic intelligence agency of the United States government. It is administered as part of the United States Department of Defense. NSA is responsible for the collection and analysis of foreign communications and foreign signals intelligence, which involves cryptanalysis. NSA is also responsible for protecting U.S. government communications and information systems from similar agencies elsewhere, which involves cryptography. NSA is a key component of the U.S. Intelligence Community, which is headed by the Director of National Intelligence. The Central Security Service is a co-located agency created to coordinate intelligence activities and co-operation between NSA and U.S. military cryptanalysis agencies. NSA's work is limited to communications intelligence. It does not perform field or human intelligence activities. Answer: B 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.

QUESTION 13
Part of your change management plan details what should happen in the change control system for your project. Theresa, a junior project manager, asks what the configuration management activities are for scope changes. You tell her that all of the following are valid configuration management activities except for which one?

A. Configuration Identification
B. Configuration Verification and Auditing
C. Configuration Status Accounting
D. Configuration Item Costing

Answer: D
Explanation:
Configuration item cost is not a valid activity for configuration management. Cost changes are managed by the cost change control system; configuration management is concerned with changes to the features and functions of the project deliverables.

QUESTION 14
Which of the following types of redundancy prevents attacks in which an attacker can get physical control of a machine, insert unauthorized software, and alter data?

A. Data redundancy
B. Hardware redundancy
C. Process redundancy
D. Application redundancy

Answer: C
Explanation:
Process redundancy permits software to run simultaneously on multiple geographically distributed locations, with voting on results. It prevents attacks in which an attacker can get physical control of a machine, insert unauthorized software, and alter data.

QUESTION 15
Which of the following individuals inspects whether the security policies, standards, guidelines, and procedures are efficiently performed in accordance with the company's stated security objectives?

A. Information system security professional
B. Data owner
C. Senior management
D. Information system auditor

Answer: D
Explanation:
An information system auditor is an individual who inspects whether the security policies, standards, guidelines, and procedures are efficiently performed in accordance with the company's stated security objectives. He is responsible for reporting the senior management about the value of security controls by performing regular and independent audits. Answer: B is incorrect. A data owner determines the sensitivity or classification levels of data. Answer: A is incorrect. An informational systems security professional is an individual who designs, implements, manages, and reviews the security policies, standards, guidelines, and procedures of the organization. He is responsible to implement and maintain security by the senior-level management. Answer: C is incorrect. A senior management assigns overall responsibilities to other individuals.

QUESTION 16
Which of the following process areas does the SSE-CMM define in the 'Project and Organizational Practices' category? Each correct answer represents a complete solution. Choose all that apply.

A. Provide Ongoing Skills and Knowledge
B. Verify and Validate Security
C. Manage Project Risk
D. Improve Organization's System Engineering Process

Answer: ACD
Explanation:
Project and Organizational Practices include the following process areas: PA12: Ensure Quality PA13: Manage Configuration PA14: Manage Project Risk PA15: Monitor and Control Technical Effort PA16: Plan Technical Effort PA17: Define Organization's System Engineering Process

PA18: Improve Organization's System Engineering Process PA19: Manage Product Line Evolution PA20: Manage Systems Engineering Support Environment PA21: Provide Ongoing Skills and Knowledge PA22: Coordinate with Suppliers

QUESTION 17
The LeGrand Vulnerability-Oriented Risk Management method is based on vulnerability analysis and consists of four principle steps. Which of the following processes does the risk assessment step include? Each correct answer represents a part of the solution. Choose all that apply.

A. Remediation of a particular vulnerability
B. Cost-benefit examination of countermeasures
C. Identification of vulnerabilities
D. Assessment of attacks

Answer: BCD
Explanation:
Risk assessment includes identification of vulnerabilities, assessment of losses caused by threats materialized, cost-benefit examination of countermeasures, and assessment of attacks. Answer: A is incorrect. This process is included in the vulnerability management.

QUESTION 18
You work as a Security Manager for Tech Perfect Inc. You have set up a SIEM server for the following purposes: Analyze the data from different log sources Correlate the events among the log entries Identify and prioritize significant events Initiate responses to events if required One of your log monitoring staff wants to know the features of SIEM product that will help them in these purposes. What features will you recommend? Each correct answer represents a complete solution. Choose all that apply.

A. Asset information storage and correlation
B. Transmission confidentiality protection
C. Incident tracking and reporting
D. Security knowledge base
E. Graphical user interface

Answer: ACDE
Explanation:
The features of SIEM products are as follows: Graphical user interface (GUI): It is used in analysis for identifying potential problems and reviewing all available data that are associated with the problems. Security knowledge base: It includes information on known vulnerabilities, log messages, and other technical data. Incident tracking and hacking: It has robust workflow features to track and report incidents. Asset information storage and correlation: It gives higher priority to an attack that affects a vulnerable OS or a main host. Answer: B is incorrect. SIEM product does not have this feature.

QUESTION 19
According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Which of the following are among the eight areas of IA defined by DoD? Each correct answer represents a complete solution. Choose all that apply.

A. VI Vulnerability and Incident Management
B. Information systems acquisition, development, and maintenance
C. DC Security Design & Configuration
D. EC Enclave and Computing Environment

Answer: ACD
Explanation:
According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Following are the various U.S. Department of Defense information security standards: DC Security Design & Configuration IA Identification and Authentication EC Enclave and Computing Environment EB Enclave Boundary Defense PE Physical and Environmental PR Personnel CO Continuity VI Vulnerability and Incident Management Answer: B is incorrect. Business continuity management is an International information security standard.

QUESTION 20
The Information System Security Officer (ISSO) and Information System Security Engineer (ISSE) play the role of a supporter and advisor, respectively. Which of the following statements are true about ISSO and ISSE? Each correct answer represents a complete solution. Choose all that apply.

A. An ISSE manages the security of the information system that is slated for Certification & Accreditation (C&A).
B. An ISSE provides advice on the continuous monitoring of the information system.
C. An ISSO manages the security of the information system that is slated for Certification & Accreditation (C&A).
D. An ISSE provides advice on the impacts of system changes.
E. An ISSO takes part in the development activities that are required to implement system changes.

Answer: BCD
Explanation:
An Information System Security Officer (ISSO) plays the role of a supporter. The responsibilities of an Information System Security Officer (ISSO) are as follows: Manages the security of the information system that is slated for Certification & Accreditation (C&A). Insures the information systems configuration with the agency's information security policy. Supports the information system owner/information owner for the completion of security-related responsibilities. Takes part in the formal configuration management process. Prepares Certification & Accreditation (C&A) packages. An Information System Security Engineer (ISSE) plays the role of an advisor. The responsibilities of an Information System Security Engineer are as follows:

Provides view on the continuous monitoring of the information system. Provides advice on the impacts of system changes. Takes part in the configuration management process. Takes part in the development activities that are required to implement system changes. Follows approved system changes.

QUESTION 21
In which of the following types of tests are the disaster recovery checklists distributed to the members of disaster recovery team and asked to review the assigned checklist?

A. Parallel test
B. Simulation test