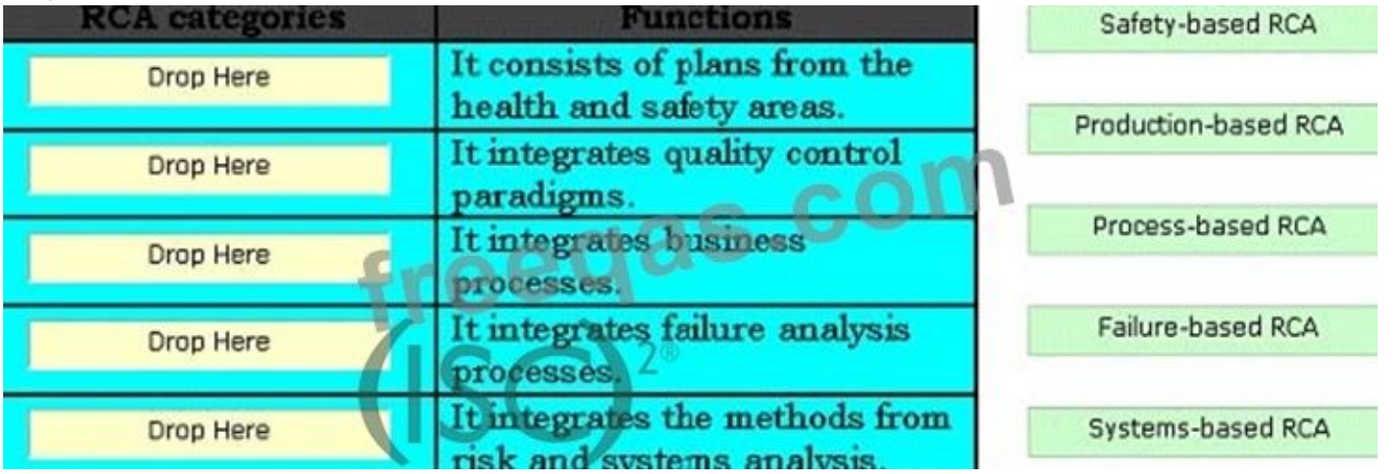
# ISC.CSSLP.v2024-03-08.q123

| | |
|---|---|
| **Exam Code:** | CSSLP |
| **Exam Name:** | Certified Secure Software Lifecycle Professional Practice Test |
| **Certification Provider:** | ISC |
| **Free Question Number:** | 123 |
| **Version:** | v2024-03-08 |
| **# of views:** | 1243 |
| **# of Questions views:** | 1230 |
| https://www.freeqas.com/qa/ISC/CSSLP/ISC.CSSLP.v2024-03-08.q123.html | |

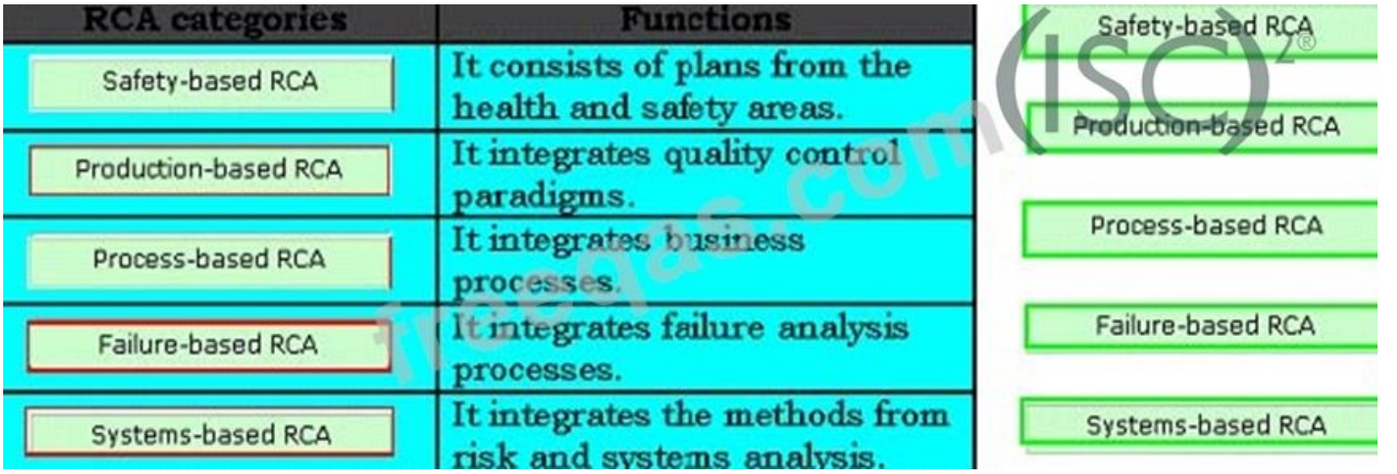
**NEW QUESTION: 1**
A number of security patterns for Web applications under the DARPA contract have been developed by Kienzle, Elder, Tyree, and Edwards-Hewitt. Which of the following patterns are applicable to aspects of authentication in Web applications?b Each correct answer represents a complete solution. Choose all that apply.
**A.** Authenticated session
**B.** Secure assertion
**C.** Partitioned application
**D.** Password authentication
**E.** Account lockout
**F.** Password propagation
**Answer: (SHOW ANSWER)**
The various patterns applicable to aspects of authentication in the Web applications are as follows: Account lockout: It implements a limit on the incorrect password attempts to protect an account from automated password-guessing attacks. Authenticated session: It allows a user to access more than one access-restricted Web page without re-authenticating every page. It also integrates user authentication into the basic session model. Password authentication: It provides protection against weak passwords, automated password-guessing attacks, and mishandling of passwords. Password propagation: It offers a choice by requiring that a user's authentication credentials be verified by the database before providing access to that user's data. Answer B and C are incorrect. Secure assertion and partitioned application patterns are applicable to software assurance in general.

**NEW QUESTION: 2**
DRAG DROP
RCA (root cause analysis) is an iterative and reactive method that identifies the root cause of various incidents, and the actions required to prevent these incidents from reoccurring. RCA is

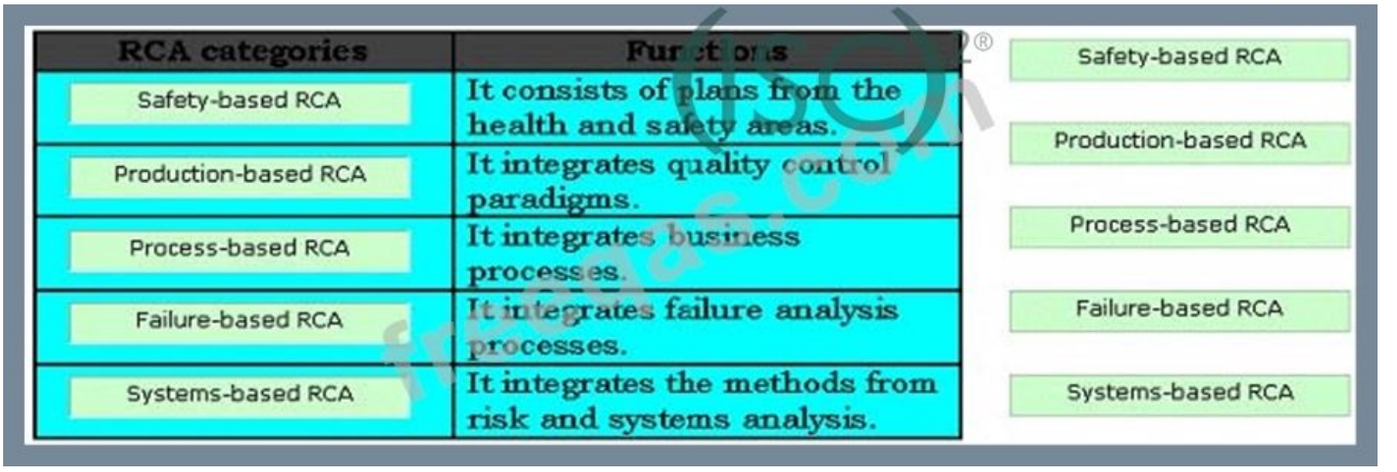
classified in various categories. Choose appropriate categories and drop them in front of their respective functions.




**Answer:**




Explanation:




The various categories of root cause analysis (RCA) are as follows: Safety-based RC A.
It consists of plans from the health and safety areas. Production-based RCA. It integrates quality control paradigms. Process-based RCA. It integrates business processes. Failure-based RCA. It integrates failure analysis processes as employed in engineering and maintenance. Systems-based RCA. It integrates the methods from risk and systems analysis.

**NEW QUESTION: 3**

Which of the following phases of the DITSCAP C&A process is used to define the C&A level of effort, to identify the main C&A roles and responsibilities, and to create an agreement on the method for implementing the security requirements?

**A.** Phase 1

**B.** Phase 4

**C.** Phase 2

**D.** Phase 3

**Answer: A (LEAVE A REPLY)**

Explanation/Reference:

Explanation: The Phase 1 of the DITSCAP C&A process 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. AnswerC is incorrect. The Phase 2 of the DITSCAP C&A process is known as Verification. Answer: D is incorrect. The Phase 3 of the DITSCAP C&A process is known as Validation. Answer: B is incorrect. The Phase 4 of the DITSCAP C&A process is known as Post Accreditation.

**NEW QUESTION: 4**

Which of the following ISO standards is entitled as "Information technology - Security techniques - Information security management - Measurement"?

**A.** ISO 27003

**B.** ISO 27005

**C.** ISO 27004

**D.** ISO 27006

**Answer: (SHOW ANSWER)**

Explanation/Reference:

Explanation: ISO 27004 is an information security standard developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is entitled as "Information technology - Security techniques - Information security management - Measurement". The ISO 27004 standard provides guidelines on specifications and use of measurement techniques for the assessment of the effectiveness of an implemented information security management system and controls. It also helps an organization in establishing the effectiveness of ISMS implementation, embracing benchmarking, and performance targeting within the PDCA (plan-do-check-act) cycle. AnswerA is incorrect. ISO 27003 is entitled as "Information Technology - Security techniques - Information security management system implementation guidance". Answer B is incorrect. ISO 27005 is entitled as "ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management". Answer: D is incorrect. ISO 27006 is entitled as "Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems".

**NEW QUESTION: 5**

Which of the following acts is used to recognize the importance of information security to the economic and national security interests of the United States?

**A.** Computer Misuse Act

**B.** Lanham Act

**C.** Computer Fraud and Abuse Act

**D.** FISMA

**Answer: D (LEAVE A REPLY)**

Explanation/Reference:

Explanation: The Federal Information Security Management Act of 2002 is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002. The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA has brought attention within the federal government to cybersecurity and explicitly emphasized a 'risk-based policy for cost-effective security'. FISMA requires agency program officials, chief information officers, and Inspectors Generals (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget (OMB). OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act. Answer:

B is incorrect. The Lanham Act is a piece of legislation that contains the federal statutes of trademark law in the United States. The Act prohibits a number of activities, including trademark infringement, trademark dilution, and false advertising. It is also called Lanham Trademark Act.

AnswerA is incorrect. The Computer Misuse Act 1990 is an act of the UK Parliament which states the following statement:

Unauthorized access to the computer material is punishable by 6 months imprisonment or a fine "not exceeding level 5 on the standard scale" (currently 5000). Unauthorized access with the intent to commit or facilitate commission of further offences is punishable by 6 months/maximum fine on summary conviction or 5 years/fine on indictment. Unauthorized modification of computer material is subject to the same sentences as section 2 offences.

AnswerC is incorrect. The Computer Fraud and Abuse Act is a law passed by the United States Congress in 1984 intended to reduce cracking of computer systems and to address federal computer- related offenses. The Computer Fraud and Abuse Act (codified as 18 U.S.C. 1030) governs cases with a compelling federal interest, where computers of the federal government or certain financial institutions are involved, where the crime itself is interstate in nature, or computers used in interstate and foreign commerce. It was amended in 1986, 1994, 1996, in 2001 by the USA PATRIOT Act, and in 2008 by the Identity Theft Enforcement and Restitution Act. Section (b) of the act punishes anyone who not just commits or attempts to commit an offense under the Computer Fraud and Abuse Act but also those who conspire to do so.

**NEW QUESTION: 6**
Which of the following are the responsibilities of the owner with regard to data in an information classification program? Each correct answer represents a complete solution. Choose three.
**A.** Reviewing the classification assignments at regular time intervals and making changes as the business needs change.
**B.** Running regular backups and routinely testing the validity of the backup data.
**C.** Delegating the responsibility of the data protection duties to a custodian.
**D.** Determining what level of classification the information requires.
**Answer: A,C,D (LEAVE A REPLY)**
The following are the responsibilities of the owner with regard to data in an information classification program: Determining what level of classification the information requires. Reviewing the classification assignments at regular time intervals and making changes as the business needs change. Delegating the responsibility of the data protection duties to a custodian. An information owner can be an executive or a manager of an organization. He will be responsible for the asset of information that must be protected. Answer B is incorrect. Running regular backups and routinely testing the validity of the backup data is the responsibility of a custodian.

**NEW QUESTION: 7**
You are the project manager of QSL project for your organization. You are working with your project team and several key stakeholders to create a diagram that shows how various elements of a system interrelate and the mechanism of causation within the system. What diagramming technique are you using as a part of the risk identification process?
**A.** Cause and effect diagrams
**B.** Influence diagrams
**C.** Predecessor and successor diagramming
**D.** System or process flowcharts
**Answer: D (LEAVE A REPLY)**
In this example you are using a system or process flowchart. These can help identify risks within the process flow, such as bottlenecks or redundancy. Answer A is incorrect. A cause and effect diagram, also known as an Ishikawa or fishbone diagram, can reveal causal factors to the effect to be solved. Answer B is incorrect. An influence diagram shows causal influences, time ordering of events and relationships among variables and outcomes. Answer C is incorrect. Predecessor and successor diagramming is not a valid risk identification term.

**NEW QUESTION: 8**
What are the various benefits of a software interface according to the "Enhancing the Development Life Cycle to Produce Secure Software" document? Each correct answer represents a complete solution. Choose three.
**A.** It modifies the implementation of a component without affecting the specifications of the interface.

**B.** It controls the accessing of a component.
**C.** It displays the implementation details of a component.
**D.** It provides a programmatic way of communication between the components that are working with different programming languages.
**Answer: A,B,D (LEAVE A REPLY)**
The benefits of a software interface are as follows: It provides a programmatic way of communication between the components that are working with different programming languages. It prevents direct communication between components. It modifies the implementation of a component without affecting the specifications of the interface. It hides the implementation details of a component. It controls the accessing of a component. Answer C is incorrect. A software interface hides the implementation details of the component.

**NEW QUESTION: 9**
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: (SHOW ANSWER)**
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.

**NEW QUESTION: 10**
You work as the Senior Project manager in Dotcoiss Inc. Your company has started a software project using configuration management and has completed 70% of it. You need to ensure that the network infrastructure devices and networking standards used in this project are installed in accordance with the requirements of its detailed project design documentation. Which of the following procedures will you employ to accomplish the task?
**A.** Configuration identification

**B.** Configuration control
**C.** Functional configuration audit
**D.** Physical configuration audit
**Answer: (SHOW ANSWER)**
Physical Configuration Audit (PCA) is one of the practices used in Software Configuration Management for Software Configuration Auditing. The purpose of the software PCA is to ensure that the design and reference documentation is consistent with the as-built software product. PCA checks and matches the really implemented layout with the documented layout. Answer C is incorrect. Functional Configuration Audit or FCA is one of the practices used in Software Configuration Management for Software Configuration Auditing. FCA occurs 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. Answer B 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 A 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.

**NEW QUESTION: 11**
Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. Which of the following statements are true about Certification and Accreditation? Each correct answer represents a complete solution. Choose two.
**A.** Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system.
**B.** Accreditation is a comprehensive assessment of the management, operational, and technical security controls in an information system.
**C.** Accreditation is the official management decision given by a senior agency official to authorize operation of an information system.
**D.** Certification is the official management decision given by a senior agency official to authorize operation of an information system.
**Answer: A,C (LEAVE A REPLY)**
Explanation/Reference:
Explanation: Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The C&A process is used extensively in the U.S. Federal Government.

Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

**NEW QUESTION: 12**
Which of the following DITSCAP phases validates that the preceding work has produced an IS that operates in a specified computing environment?
**A.** Phase 2
**B.** Phase 4
**C.** Phase 1
**D.** Phase 3
**Answer: (SHOW ANSWER)**
Explanation/Reference:
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. AnswerC is incorrect. 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.
AnswerA is incorrect. The goal of this phase is to obtain a fully integrated system for certification testing
and accreditation. AnswerB is incorrect. This phase ensures that it will maintain an acceptable level of residual risk.

**NEW QUESTION: 13**
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 (LEAVE A REPLY)**
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.

**NEW QUESTION: 14**
Which of the following governance bodies provides management, operational and technical controls to satisfy security requirements?
**A.** Senior Management
**B.** Business Unit Manager
**C.** Information Security Steering Committee
**D.** Chief Information Security Officer
**Answer: A (LEAVE A REPLY)**
Senior management provides management, operational and technical controls to satisfy security requirements. The governance roles and responsibilities are mentioned below in the table:

| Governance Body | Membership | Responsibilities |
|---|---|---|
| Information Security Steering Commitee | CFO, CEO, COO, CTO, VP Business units chaired by CISO | It establishes and supports security programs |
| Senior Management | C-level, unit VPs and senior VPs | It provides management, operational and technical controls to satisfy security requirements. |
| Chief Information Security Officer | CISO and staff | It directs and coordinates implementations of information security program. |
| Business Unit Managers | Department heads and supervisors | They Classify and establish requirements for safeguarding information assets. |

**NEW QUESTION: 15**
Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?
**A.** Single Loss Expectancy (SLE)
**B.** Annualized Rate of Occurrence (ARO)
**C.** Safeguard
**D.** Exposure Factor (EF)
**Answer: B (LEAVE A REPLY)**
The Annualized Rate of Occurrence (ARO) is a number that represents the estimated frequency at which a threat is expected to occur. It is calculated based upon the probability of the event occurring and the number of employees that could make that event occur. Answer D is incorrect. The Exposure Factor (EF) represents the % of assets loss caused by a threat. The EF is required to calculate the Single Loss Expectancy (SLE). Answer A is incorrect. The Single Loss

Expectancy (SLE) is the value in dollars that is assigned to a single event. SLE = Asset Value ($) X Exposure Factor (EF) Answer C is incorrect. Safeguard acts as a countermeasure for reducing the risk associated with a specific threat or a group of threats.

**NEW QUESTION: 16**
Which of the following DoD directives is referred to as the Defense Automation Resources Management Manual?
**A.** DoD 8910.1
**B.** DoD 7950.1-M
**C.** DoDD 8000.1
**D.** DoD 5200.22-M
**E.** DoD 5200.1-R
**Answer: B (LEAVE A REPLY)**
Explanation/Reference:
Explanation: The various DoD directives are as follows:
DoD 5200.1-R: This DoD directive refers to the 'Information Security Program Regulation'. DoD 5200.22- M: This DoD directive refers the 'National Industrial Security Program Operating Manual'. 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'.



**NEW QUESTION: 17**
Audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function. Under which of the following controls does audit control come?
**A.** Reactive controls
**B.** Detective controls
**C.** Protective controls
**D.** Preventive controls
**Answer: B (LEAVE A REPLY)**

Audit trail or audit log comes under detective controls. Detective controls are the audit controls that are not needed to be restricted. Any control that performs a monitoring activity can likely be defined as a Detective Control. For example, it is possible that mistakes, either intentional or unintentional, can be made. Therefore, an additional Protective control is that these companies must have their financial results audited by an independent Certified Public Accountant. The role of this accountant is to act as an auditor. In fact, any auditor acts as a Detective control. If the organization in question has not properly followed the rules, a diligent auditor should be able to detect the deficiency which indicates that some control somewhere has failed. Answer A is incorrect. Reactive or corrective controls typically work in response to a detective control, responding in such a way as to alert or otherwise correct an unacceptable condition. Using the example of account rules, either the internal Audit Committee or the SEC itself, based on the report generated by the external auditor, will take some corrective action. In this way, they are acting as a Corrective or Reactive control. Answer C and D are incorrect. Protective or preventative controls serve to proactively define and possibly enforce acceptable behaviors. As an example, a set of common accounting rules are defined and must be followed by any publicly traded company. Each quarter, any particular company must publicly state its current financial standing and accounting as reflected by an application of these rules. These accounting rules and the SEC requirements serve as protective or preventative controls.

**NEW QUESTION: 18**
What component of the change management system is responsible for evaluating, testing, and documenting changes created to the project scope?
**A.** Project Management Information System
**B.** Integrated Change Control
**C.** Configuration Management System
**D.** Scope Verification
**Answer: C (LEAVE A REPLY)**
The change management system is comprised of several components that guide the change request through the process. When a change request is made that will affect the project scope. The Configuration Management System evaluates the change request and documents the features and functions of the change on the project scope.

**NEW QUESTION: 19**
Which of the following are the primary functions of configuration management? Each correct answer represents a complete solution. Choose all that apply.
**A.** It removes the risk event entirely by adding additional steps to avoid the event.
**B.** It ensures that the change is implemented in a sequential manner through formalized testing.
**C.** It reduces the negative impact that the change might have had on the computing services and resources.
**D.** It analyzes the effect of the change that is implemented on the system.
**Answer: (SHOW ANSWER)**

The primary functions of configuration management are as follows: It ensures that the change is implemented in a sequential manner through formalized testing. It ensures that the user base is informed of the future change. It analyzes the effect of the change that is implemented on the system. It reduces the negative impact that the change might have had on the computing services and resources. Answer A is incorrect. It is not one of the primary functions of configuration management. It is the function of risk avoidance.

**NEW QUESTION: 20**
Which of the following methods can be helpful to eliminate social engineering threat? Each correct answer represents a complete solution. Choose three.
**A.** Password policies
**B.** Data classification
**C.** Data encryption
**D.** Vulnerability assessments
**Answer: A,B,D (LEAVE A REPLY)**
The following methods can be helpful to eliminate social engineering threat: Password policies Vulnerability assessments Data classification Password policy should specify that how the password can be shared. Company should implement periodic penetration and vulnerability assessments. These assessments usually consist of using known hacker tools and common hacker techniques to breach a network security. Social engineering should also be used for an accurate assessment. Since social engineers use the knowledge of others to attain information, it is essential to have a data classification model in place that all employees know and follow. Data classification assigns level of sensitivity of company information. Each classification level specifies that who can view and edit data, and how it can be shared.

**NEW QUESTION: 21**
The service-oriented modeling framework (SOMF) provides a common modeling notation to address alignment between business and IT organizations. Which of the following principles does the SOMF concentrate on? Each correct answer represents a part of the solution. Choose all that apply.
**A.** Architectural components abstraction
**B.** SOA value proposition
**C.** Business traceability
**D.** Disaster recovery planning
**E.** Software assets reuse
**Answer: A,B,C,E (LEAVE A REPLY)**
Explanation/Reference:
Explanation: The service-oriented modeling framework (SOMF) concentrates on the following principles:
Business traceability Architectural best-practices traceability Technological traceability SOA value proposition Software assets reuse SOA integration strategies Technological abstraction and

generalization Architectural components abstraction Answer: D is incorrect. The service-oriented modeling framework (SOMF) does not concentrate on it.

**NEW QUESTION: 22**
The DARPA paper defines various procedural patterns to perform secure system development practices. Which of the following patterns does it include? Each correct answer represents a complete solution. Choose three.
**A.** Hidden implementation
**B.** Document the server configuration
**C.** Patch proactively
**D.** Red team the design
**E.** Password propagation
**Answer: B,C,D (LEAVE A REPLY)**
The following procedural patterns are defined by the DARPA paper in order to perform secure software development practices: Build the server from the ground up: It includes the following features: Build the server from the ground up. Identify the default installation of the operating system and applications. Support hardening procedures to remove unnecessary services. Identify a vulnerable service for ongoing risk management. Choose the right stuff: It defines guidelines to select right commercial off-the-shelf (COTS) components and decide whether to use and build custom components. Document the server configuration: It supports the creation of an initial configuration baseline and tracks all modifications made to servers and application configurations. Patch proactively: It supports in applying patches as soon as they are available rather than waiting until the systems cooperate. Red team the design: It supports an independent security assessment from the perspective of an attacker in the quality assurance or testing stage. An independent security assessment is helpful in addressing a security issue before it occurs. Answer A is incorrect. Hidden implementation pattern is not defined in the DARPA paper. This pattern is applicable to software assurance in general. Hidden implementation limits the ability of an attacker to distinguish the internal workings of an application. Answer E is incorrect. Password propagation is not defined in the DARPA paper. This pattern is applicable to aspects of authentication in a Web application. Password propagation provides an alternative by requiring that a user's authentication credentials be verified by the database before providing access to that user's data.

**NEW QUESTION: 23**
DoD 8500.2 establishes IA controls for information systems according to the Mission Assurance Categories (MAC) and confidentiality levels. Which of the following MAC levels requires high integrity and medium availability?
**A.** MAC III
**B.** MAC IV
**C.** MAC I
**D.** MAC II

**Answer: D (LEAVE A REPLY)**
The various MAC levels are as follows: MAC I: It states that the systems have high availability and high integrity. MAC II: It states that the systems have high integrity and medium availability. MAC III: It states that the systems have basic integrity and availability.

**NEW QUESTION: 24**
Fill in the blank with an appropriate phrase. A is defined as any activity that has an effect on defining, designing, building, or executing a task, requirement, or procedure.
**A.** technical effort
**Answer: A (LEAVE A REPLY)**
A technical effort is described as any activity, which has an effect on defining, designing, building, or implementing a task, requirement, or procedure. The technical effort is an element of technical management that is required to progress efficiently and effectively from a business need to the deployment and operation of the system.

**NEW QUESTION: 25**
Which of the following statements reflect the 'Code of Ethics Canons' in the '(ISC)2 Code of Ethics'? Each correct answer represents a complete solution. Choose all that apply.
**A.** Act honorably, honestly, justly, responsibly, and legally.
**B.** Give guidance for resolving good versus good and bad versus bad dilemmas.
**C.** Provide diligent and competent service to principals.
**D.** Protect society, the commonwealth, and the infrastructure.
**Answer: A,C,D (LEAVE A REPLY)**
The Code of Ethics Canons in (ISC)2 code of ethics are as follows: Protect society, the commonwealth, and the infrastructure. Act honorably, honestly, justly, responsibly, and legally.
Provide diligent and competent service to principals. Advance and protect the profession.

**NEW QUESTION: 26**
Which of the following terms ensures that no intentional or unintentional unauthorized modification is made to data?
**A.** Non-repudiation
**B.** Integrity
**C.** Authentication
**D.** Confidentiality
**Answer: (SHOW ANSWER)**
Explanation/Reference:
Explanation: Integrity ensures that no intentional or unintentional unauthorized modification is made to data. Answer: D is incorrect. Confidentiality refers to the protection of data against unauthorized access.

Administrators can provide confidentiality by encrypting data. Answer: A is incorrect. Non-repudiation is a mechanism to prove that the sender really sent this message. Answer: C is incorrect. Authentication is the process of verifying the identity of a person or network host.

**NEW QUESTION: 27**
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 (LEAVE A REPLY)**
Explanation/Reference:
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.

**NEW QUESTION: 28**
Which of the following programming languages are compiled into machine code and directly executed by the CPU of a computer system? Each correct answer represents a complete solution. Choose two.
**A.** C
**B.** Microosft.NET
**C.** Java EE
**D.** C++
**Answer: A,D (LEAVE A REPLY)**
C and C++ programming languages are unmanaged code. Unmanaged code is compiled into machine code and directly executed by the CPU of a computer system. Answer C and B are incorrect. Java EE and Microsoft.Net are compiled into an intermediate code format.

**NEW QUESTION: 29**
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: A,C,D,E (LEAVE A REPLY)**

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.

**NEW QUESTION: 30**

Security controls are safeguards or countermeasures to avoid, counteract, or minimize security risks. Which of the following are types of security controls? Each correct answer represents a complete solution. Choose all that apply.

**A.** Common controls

**B.** Hybrid controls

**C.** Storage controls

**D.** System-specific controls

**E.** Explanation:

Security controls are safeguards or countermeasures to avoid, counteract, or minimize security risks. The following are the types of security controls for information systems, that can be employed by an organization: 1.System-specific controls: These types of security controls provide security capability for a particular information system only. 2.Common controls: These types of security controls provide security capability for multiple information systems. 3.Hybrid controls: These types of security controls have features of both system-specific and common controls.

**Answer: (SHOW ANSWER)**

is incorrect. It is an invalid control.

**NEW QUESTION: 31**

Audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function. Under which of the following controls does audit control come?

**A.** Reactive controls

**B.** Detective controls
**C.** Protective controls
**D.** Preventive controls
**Answer: B (LEAVE A REPLY)**
Explanation/Reference:
Explanation: Audit trail or audit log comes under detective controls. Detective controls are the audit controls that are not needed to be restricted. Any control that performs a monitoring activity can likely be defined as a Detective Control. For example, it is possible that mistakes, either intentional or unintentional, can be made. Therefore, an additional Protective control is that these companies must have their financial results audited by an independent Certified Public Accountant. The role of this accountant is to act as an auditor. In fact, any auditor acts as a Detective control. If the organization in question has not properly followed the rules, a diligent auditor should be able to detect the deficiency which indicates that some control somewhere has failed. AnswerA is incorrect. Reactive or corrective controls typically work in response to a detective control, responding in such a way as to alert or otherwise correct an unacceptable condition. Using the example of account rules, either the internal Audit Committee or the SEC itself, based on the report generated by the external auditor, will take some corrective action. In this way, they are acting as a Corrective or Reactive control. AnswerC and D are incorrect. Protective or preventative controls serve to proactively define and possibly enforce acceptable behaviors. As an example, a set of common accounting rules are defined and must be followed by any publicly traded company. Each quarter, any particular company must publicly state its current financial standing and accounting as reflected by an application of these rules. These accounting rules and the SEC requirements serve as protective or preventative controls.



**NEW QUESTION: 32**
You are responsible for network and information security at a large hospital. It is a significant concern that any change to any patient record can be easily traced back to the person who made that change. What is this called?
**A.** Availability
**B.** Confidentiality
**C.** Non repudiation
**D.** Data Protection

**Answer: (SHOW ANSWER)**
Explanation/Reference:
Explanation: Non repudiation refers to mechanisms that prevent a party from falsely denying involvement in some data transaction.

**NEW QUESTION: 33**
You work as a Security Manager for Tech Perfect Inc. You find that some applications have failed to encrypt network traffic while ensuring secure communications in the organization. Which of the following will you use to resolve the issue?
**A.** SCP
**B.** TLS
**C.** IPSec
**D.** HTTPS
**Answer: B (LEAVE A REPLY)**
Explanation/Reference:
Explanation: In order to resolve the issue, you should use TLS (Transport Layer Security). Transport Layer Security (TLS) is a cryptographic protocol that provides security and data integrity for communications over networks such as the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end. Several versions of the protocols are in wide-spread use in applications like web browsing, electronic mail, Internet faxing, instant messaging, and voice-over-IP (VoIP). The TLS protocol, an application layer protocol, allows client/server applications to communicate across a network in a way designed to prevent eavesdropping, tampering, and message forgery. TLS provides endpoint authentication and communications confidentiality over the Internet using cryptography. AnswerC is incorrect. Internet Protocol Security (IPSec) is a method of securing data. It secures traffic by using encryption and digital signing. It enhances the security of data as if an IPSec packet is captured, its contents cannot be read. IPSec also provides sender verification that ensures the certainty of the datagram's origin to the receiver. Answer D is incorrect. Hypertext Transfer Protocol Secure (HTTPS) protocol is a protocol used in the Universal Resource Locater (URL) address line to connect to a secure site. If a site has been made secure by using the Secure Sockets Layer (SSL) then HTTPS, instead of HTTP protocol, should be used as a protocol type in the URL. Answer: A is incorrect. The SCP (secure copy) protocol is a network protocol that supports file transfers. The SCP protocol, which runs on port 22, is based on the BSD RCP protocol which is tunneled through the Secure Shell (SSH) protocol to provide encryption and authentication. SCP might not even be considered a protocol itself, but merely a combination of RCP and SSH. The RCP protocol performs the file transfer and the SSH protocol performs authentication and encryption. SCP protects the authenticity and confidentiality of the data in transit. It hinders the ability for packet sniffers to extract usable information from the data packets.

**NEW QUESTION: 34**

Which of the following is used by attackers to record everything a person types, including usernames, passwords, and account information?

**A.** Packet sniffing

**B.** Keystroke logging

**C.** Spoofing

**D.** Wiretapping

**Answer: B (LEAVE A REPLY)**

Keystroke logging is used by attackers to record everything a person types, including usernames, passwords, and account information. Keystroke logging is a method of logging and recording user keystrokes. It can be performed with software or hardware devices. Keystroke logging devices can record everything a person types using his keyboard, such as to measure employee's productivity on certain clerical tasks. These types of devices can also be used to get usernames, passwords, etc. Answer D is incorrect. Wiretapping is used to eavesdrop on voice calls. Eavesdropping is the process of listening in on private conversations. It also includes attackers listening in on network traffic. Answer C is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected. Answer A is incorrect. Packet sniffing is a process of monitoring data packets that travel across a network. The software used for packet sniffing is known as sniffers. There are many packet-sniffing programs that are available on the Internet. Some of these are unauthorized, which can be harmful for a network's security.

**NEW QUESTION: 35**

Which of the following security design patterns provides an alternative by requiring that a user's authentication credentials be verified by the database before providing access to that user's data?

**A.** Secure assertion

**B.** Authenticated session

**C.** Password propagation

**D.** Account lockout

**Answer: C (LEAVE A REPLY)**

Password propagation provides an alternative by requiring that a user's authentication credentials be verified by the database before providing access to that user's data. Answer D is incorrect. Account lockout implements a limit on the incorrect password attempts to protect an account from automated password-guessing attacks. Answer B is incorrect. Authenticated session allows a user to access more than one access-restricted Web page without re-authenticating every page. It also integrates user authentication into the basic session model. Answer A is incorrect. Secure assertion distributes application-specific sanity checks throughout the system.

**NEW QUESTION: 36**

Gary is the project manager for his project. He and the project team have completed the qualitative risk analysis process and are about to enter the quantitative risk analysis process when Mary, the project sponsor, wants to know what quantitative risk analysis will review. Which of the following statements best defines what quantitative risk analysis will review?
**A.** The quantitative risk analysis process will analyze the effect of risk events that may substantially impact the project's competing demands.
**B.** The quantitative risk analysis reviews the results of risk identification and prepares the project for risk response management.
**C.** The quantitative risk analysis seeks to determine the true cost of each identified risk event and the probability of each risk event to determine the risk exposure.
**D.** The quantitative risk analysis process will review risk events for their probability and impact on the project objectives.
**Answer: A (LEAVE A REPLY)**
Once the risk events have passed through qualitative risk analysis, then the risk events must be reviewed to determine the effect of the risks on the project's competing demands. Answer D is incorrect. While the quantitative risk analysis process will review the risk events for probability and impact, this statement does not answer the question as completely as answer option A.
Answer C is incorrect. The quantitative risk analysis process does not review every risk identified - only the risks which require further analysis. Answer B is incorrect. Quantitative risk analysis process does not begin the risk response process. Its goal is to determine the effect of certain risk events on the project's competing demands.

**NEW QUESTION: 37**
The service-oriented modeling framework (SOMF) introduces five major life cycle modeling activities that drive a service evolution during design-time and run-time. Which of the following activities integrates SOA software assets and establishes SOA logical environment dependencies?
**A.** Service-oriented discovery and analysis modeling
**B.** Service-oriented business integration modeling
**C.** Service-oriented logical architecture modeling
**D.** Service-oriented logical design modeling
**Answer: C (LEAVE A REPLY)**
Explanation/Reference:
Explanation: The service-oriented logical architecture modeling integrates SOA software assets and establishes SOA logical environment dependencies. It also offers foster service reuse, loose coupling and consolidation. AnswerA is incorrect. The service-oriented discovery and analysis modeling discovers and analyzes services for granularity, reusability, interoperability, loose-coupling, and identifies consolidation opportunities. Answer B is incorrect. The service-oriented business integration modeling identifies service integration and alignment opportunities with business domains' processes. Answer: D is incorrect. The service-oriented logical design modeling establishes service relationships and message exchange paths.

**NEW QUESTION: 38**
Which of the following recovery plans includes specific strategies and actions to deal with specific variances to assumptions resulting in a particular security problem, emergency, or state of affairs?
**A.** Disaster recovery plan
**B.** Business continuity plan
**C.** Continuity of Operations Plan
**D.** Contingency plan
**Answer: D (LEAVE A REPLY)**
A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and triggers for initiating planned actions. Answer A is incorrect. Disaster recovery is the process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Answer B is incorrect. It deals with the plans and procedures that identify and prioritize the critical business functions that must be preserved. Answer C is incorrect. It includes the plans and procedures documented that ensure the continuity of critical operations during any period where normal operations are impossible.

**NEW QUESTION: 39**
Which of the following are examples of the application programming interface (API)? Each correct answer represents a complete solution. Choose three.
**A.** HTML
**B.** PHP
**C.** .NET
**D.** Perl
**Answer: B,C,D (LEAVE A REPLY)**
Explanation/Reference:
Explanation: Perl, .NET, and PHP are examples of the application programming interface (API). API is a set of routines, protocols, and tools that users can use to work with a component, application, or operating system. It consists of one or more DLLs that provide specific functionality. API helps in reducing the development time of applications by reducing application code. Most operating environments, such as MS- Windows, provide an API so that programmers can write applications consistent with the operating environment. Answer: A is incorrect. HTML stands for Hypertext Markup Language. It is a set of markup symbols or codes used to create Web pages and define formatting specifications. The markup tells the Web browser how to display the content of the Web page.

**NEW QUESTION: 40**

Penetration testing (also called pen testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit. Which of the following areas can be exploited in a penetration test? Each correct answer represents a complete solution. Choose all that apply.

**A.** Kernel flaws
**B.** Information system architectures
**C.** Race conditions
**D.** File and directory permissions
**E.** Buffer overflows
**F.** Trojan horses
**G.** Social engineering

**Answer: A,C,D,E,F,G (LEAVE A REPLY)**

Explanation/Reference:

Explanation: Penetration testing (also called pen testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit. Following are the areas that can be exploited in a penetration test: Kernel flaws: Kernel flaws refer to the exploitation of kernel code flaws in the operating system. Buffer overflows: Buffer overflows refer to the exploitation of a software failure to properly check for the length of input data. This overflow can cause malicious behavior on the system. Race conditions: A race condition is a situation in which an attacker can gain access to a system as a privileged user. File and directory permissions: In this area, an attacker exploits weak permissions restrictions to gain unauthorized access of documents. Trojan horses: These are malicious programs that can exploit an information system by attaching themselves in valid programs and files. Social engineering: In this technique, an attacker uses his social skills and persuasion to acquire valuable information that can be used to conduct an attack against a system.

**NEW QUESTION: 41**

What project management plan is most likely to direct the quantitative risk analysis process for a project in a matrix environment?

**A.** Risk analysis plan
**B.** Staffing management plan
**C.** Risk management plan
**D.** Human resource management plan

**Answer: C (LEAVE A REPLY)**

Explanation/Reference:

Explanation: The risk management plan defines how risks will be identified, analyzed, responded to, and then monitored and controlled regardless of the structure of the organization. AnswerD is incorrect. The human resources management plan does define how risks will be analyzed. Answer: B is incorrect. The staffing management plan does define how risks will be analyzed. Answer: A is incorrect. The risk analysis plan does define how risks will be analyzed.

**NEW QUESTION: 42**
Fill in the blank with an appropriate phrase. is used to provide security mechanisms for the storage, processing, and transfer of data.
**A.** Data classification
**Answer: A (LEAVE A REPLY)**
Data classification is used to protect the data based on its sensitivity, secrecy, and confidentiality. It provides security mechanisms for storage, processing, and transfer of data. Data classification also helps to verify the effort, funds, and resources allocated to save the data, and controls access to it.

**NEW QUESTION: 43**
You work as a Security Manager for Tech Perfect Inc. You find that some applications have failed to encrypt network traffic while ensuring secure communications in the organization. Which of the following will you use to resolve the issue?
**A.** SCP
**B.** TLS
**C.** IPSec
**D.** HTTPS
**Answer: B (LEAVE A REPLY)**
In order to resolve the issue, you should use TLS (Transport Layer Security). Transport Layer Security (TLS) is a cryptographic protocol that provides security and data integrity for communications over networks such as the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end. Several versions of the protocols are in wide-spread use in applications like web browsing, electronic mail, Internet faxing, instant messaging, and voice-over-IP (VoIP). The TLS protocol, an application layer protocol, allows client/server applications to communicate across a network in a way designed to prevent eavesdropping, tampering, and message forgery. TLS provides endpoint authentication and communications confidentiality over the Internet using cryptography. Answer C is incorrect. Internet Protocol Security (IPSec) is a method of securing data. It secures traffic by using encryption and digital signing. It enhances the security of data as if an IPSec packet is captured, its contents cannot be read. IPSec also provides sender verification that ensures the certainty of the datagram's origin to the receiver. Answer D is incorrect. Hypertext Transfer Protocol Secure (HTTPS) protocol is a protocol used in the Universal Resource Locater (URL) address line to connect to a secure site. If a site has been made secure by using the Secure Sockets Layer (SSL) then HTTPS, instead of HTTP protocol, should be used as a protocol type in the URL. Answer A is incorrect. The SCP (secure copy) protocol is a network protocol that supports file transfers. The SCP protocol, which runs on port 22, is based on the BSD RCP protocol which is tunneled through the Secure Shell (SSH) protocol to provide encryption and authentication. SCP might not even be considered a protocol itself, but merely a combination of RCP and SSH. The RCP protocol performs the file transfer and the SSH protocol performs authentication and

encryption. SCP protects the authenticity and confidentiality of the data in transit. It hinders the ability for packet sniffers to extract usable information from the data packets.

**NEW QUESTION: 44**
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: A,B,D (LEAVE A REPLY)**
Explanation/Reference:
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. AnswerC is incorrect. Financial assessment does not come under the ISO/IEC 27002 standard.

**NEW QUESTION: 45**
Which of the following security models characterizes the rights of each subject with respect to every object in the computer system?
**A.** Clark-Wilson model
**B.** Bell-LaPadula model
**C.** Biba model
**D.** Access matrix
**Answer: (SHOW ANSWER)**

The access matrix or access control matrix is an abstract, formal security model of protection state in computer systems that characterizes the rights of each subject with respect to every object in the system. It was first introduced by Butler W.
Lampson in 1971. According to the access matrix model, the protection state of a computer system can be abstracted as a set of objects 'O', that is the set of entities that needs to be protected (e.g. processes, files, memory pages) and a set of subjects 'S' that consists of all active entities (e.g. users, processes). Further there exists a set of rights 'R' of the form r(s,o), where s S, o O and r(s,o) R.
A right thereby specifies the kind of access a subject is allowed to process with regard to an object. Answer B is incorrect. The Bell-La Padula Model is a state machine model used for enforcing access control in government and military applications. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g.,"Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public"). The Bell-La Padula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity. Answer A is incorrect. The Clark-Wilson model provides a foundation for specifying and analyzing an integrity policy for a computing system. The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. The model's enforcement and certification rules define data items and processes that provide the basis for an integrity policy. The core of the model is based on the notion of a transaction. Answer C is incorrect. 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.

**NEW QUESTION: 46**
Single Loss Expectancy (SLE) represents an organization's loss from a single threat. Which of the following formulas best describes the Single Loss Expectancy (SLE)?
**A.** SLE = Asset Value (AV) * Exposure Factor (EF)
**B.** SLE = Annualized Loss Expectancy (ALE) * Annualized Rate of Occurrence (ARO)
**C.** SLE = Annualized Loss Expectancy (ALE) * Exposure Factor (EF)
**D.** SLE = Asset Value (AV) * Annualized Rate of Occurrence (ARO)
**Answer: A (LEAVE A REPLY)**
Explanation/Reference:
Explanation: Single Loss Expectancy is a term related to Risk Management and Risk Assessment. It can be defined as the monetary value expected from the occurrence of a risk on an asset. It is mathematically expressed as follows: Single Loss Expectancy (SLE) = Asset Value (AV) * Exposure Factor (EF) where the Exposure Factor is represented in the impact of the risk

over the asset, or percentage of asset lost. As an example, if the Asset Value is reduced two thirds, the exposure factor value is .66. If the asset is completely lost, the Exposure Factor is 1.0. The result is a monetary value in the same unit as the Single Loss Expectancy is expressed. AnswerC, D, and B are incorrect. These are not valid formulas of SLE.



**NEW QUESTION: 47**
The build environment of secure coding consists of some tools that actively support secure specification, design, and implementation. Which of the following features do these tools have? Each correct answer represents a complete solution. Choose all that apply.
**A.** They decrease the exploitable flaws and weaknesses.
**B.** They reduce and restrain the propagation, extent, and damage that have occurred by insecure software behavior.
**C.** They decrease the attack surface.
**D.** They employ software security constraints, protections, and services.
**E.** They decrease the level of type checking and program analysis.
**Answer: A,B,C,D (LEAVE A REPLY)**
The tools that produce secure software have the following features: They decrease the exploitable flaws and weaknesses. They decrease the attack surface. They employ software security constraints, protections, and services. They reduce and restrain the propagation, extent, and damage that are caused by the behavior of insecure software. Answer E is incorrect. This feature is not required for these tools.

**NEW QUESTION: 48**
Which of the following test methods has the objective to test the IT system from the viewpoint of a threat- source and to identify potential failures in the IT system protection schemes?
**A.** Security Test and Evaluation (ST&E)
**B.** Penetration testing
**C.** Automated vulnerability scanning tool
**D.** On-site interviews
**Answer: (SHOW ANSWER)**
Explanation/Reference:

Explanation: The goal of penetration testing is to examine the IT system from the perspective of a threat- source, and to identify potential failures in the IT system protection schemes. Penetration testing, when performed in the risk assessment process, is used to assess an IT system's capability to survive with the intended attempts to thwart system security. AnswerA is incorrect. The objective of ST&E is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards.

**NEW QUESTION: 49**
Which of the following DITSCAP C&A phases takes place between the signing of the initial version of the SSAA and the formal accreditation of the system?
**A.** Phase 4
**B.** Phase 3
**C.** Phase 1
**D.** Phase 2
**Answer: D (LEAVE A REPLY)**
Explanation/Reference:
Explanation: 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. Answer: C, B, and A are incorrect. These phases do not take place between the signing of the initial version of the SSAA and the formal accreditation of the system.

**NEW QUESTION: 50**
An authentication method uses smart cards as well as usernames and passwords for authentication. Which of the following authentication methods is being referred to?
**A.** Anonymous
**B.** Mutual
**C.** Multi-factor
**D.** Biometrics
**Answer: C (LEAVE A REPLY)**
Multi-factor authentication involves a combination of multiple methods of authentication. For example, an authentication method that uses smart cards as well as usernames and passwords can be referred to as multi-factor authentication. Answer B is incorrect. Mutual authentication is a process in which a client process and server are required to prove their identities to each other before performing any application function. The client and server identities can be verified through a trusted third party and use shared secrets as in the case of Kerberos v5. The MS-CHAP v2 and EAP-TLS authentication methods support mutual authentication. Answer A is incorrect. Anonymous authentication is an authentication method used for Internet communication. It provides limited access to specific public folders and directory information. It is supported by all

clients and is used to access unsecured content in public folders. An administrator must create a user account in IIS to enable the user to connect anonymously. Answer D is incorrect. Biometrics authentication uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user.

**NEW QUESTION: 51**
Which of the following cryptographic system services ensures that information will not be disclosed to any unauthorized person on a local network?
**A.** Authentication
**B.** Integrity
**C.** Non-repudiation
**D.** Confidentiality
**Answer: D (LEAVE A REPLY)**
The confidentiality service of a cryptographic system ensures that information will not be disclosed to any unauthorized person on a local network.

**NEW QUESTION: 52**
Which of the following terms refers to the protection of data against unauthorized access?
**A.** Integrity
**B.** Recovery
**C.** Auditing
**D.** Confidentiality
**Answer: D (LEAVE A REPLY)**
Confidentiality is a term that refers to the protection of data against unauthorized access. Administrators can provide confidentiality by encrypting data. Symmetric encryption is a relatively fast encryption method. Hence, this method of encryption is best suited for encrypting large amounts of data such as files on a computer. Answer A is incorrect. Integrity ensures that no intentional or unintentional unauthorized modification is made to data. Answer C is incorrect. Auditing is used to track user accounts for file and object access, logon attempts, system shutdown etc. This enhances the security of the network. Before enabling auditing, the type of event to be audited should be specified in the Audit Policy in User Manager for Domains.

**NEW QUESTION: 53**
You and your project team have identified the project risks and now are analyzing the probability and impact of the risks. What type of analysis of the risks provides a quick and high-level review of each identified risk event?
**A.** Quantitative risk analysis
**B.** Qualitative risk analysis
**C.** Seven risk responses
**D.** A risk probability-impact matrix
**Answer: B (LEAVE A REPLY)**

Explanation/Reference:
Explanation: Qualitative risk analysis is a high-level, fast review of the risk event. Qualitative risk analysis qualifies the risk events for additional analysis.

**NEW QUESTION: 54**
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: B,C,D (LEAVE A REPLY)**
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.

**NEW QUESTION: 55**
Which of the following are the responsibilities of a custodian with regard to data in an information classification program? Each correct answer represents a complete solution. Choose three.
**A.** Performing data restoration from the backups when necessary
**B.** Running regular backups and routinely testing the validity of the backup data
**C.** Determining what level of classification the information requires
**D.** Controlling access, adding and removing privileges for individual users
**Answer: A,B,D (LEAVE A REPLY)**
The owner of information delegates the responsibility of protecting that information to a custodian. The following are the responsibilities of a custodian with regard to data in an information classification program: Running regular backups and routinely testing the validity of the backup data Performing data restoration from the backups when necessary Controlling access, adding and removing privileges for individual users Answer C is incorrect. Determining what level of classification the information requires is the responsibility of the owner.

**NEW QUESTION: 56**

The Systems Development Life Cycle (SDLC) is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems. Which of the following are the different phases of system development life cycle? Each correct answer represents a complete solution.
Choose all that apply.
**A.** Testing
**B.** Implementation
**C.** Operation/maintenance
**D.** Development/acquisition
**E.** Disposal
**F.** Initiation
**Answer: (SHOW ANSWER)**
Explanation/Reference:
Explanation: The Systems Development Life Cycle (SDLC), or Software Development Life Cycle in systems engineering, information systems, and software engineering, is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems. The concept generally refers to computers or information systems. The following are the five phases in a generic System Development Life Cycle: 1.Initiation 2.Development/acquisition 3.Implementation 4.Operation/ maintenance 5.Disposal

**NEW QUESTION: 57**
Which of the following rated systems of the Orange book has mandatory protection of the TCB?
**A.** A-rated
**B.** B-rated
**C.** D-rated
**D.** C-rated
**Answer: B (LEAVE A REPLY)**
Explanation/Reference:
Explanation: A B-rated system of the orange book has mandatory protection of the trusted computing base (TCB).
Trusted computing base (TCB) refers to hardware, software, controls, and processes that cause a computer system or network to be devoid of malicious software or hardware. Maintaining the trusted computing base (TCB) is essential for security policy to be implemented successfully.

**NEW QUESTION: 58**
Which of the following processes culminates in an agreement between key players that a system in its current configuration and operation provides adequate protection controls?
**A.** Information Assurance (IA)
**B.** Information systems security engineering (ISSE)
**C.** Certification and accreditation (C&A)
**D.** Risk Management

**Answer: (SHOW ANSWER)**

Explanation/Reference:

Explanation: Certification and accreditation (C&A) is a set of processes that culminate in an agreement between key players that a system in its current configuration and operation provides adequate protection controls. Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The C&A process is used extensively in the U.S. Federal Government. Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed- upon set of security controls. Answer: D is incorrect. Risk management is a set of processes that ensures a risk-based approach is used to determine adequate, cost- effective security for a system. Answer: A is incorrect. Information assurance (IA) is the process of organizing and monitoring information-related risks.

It ensures that only the approved users have access to the approved information at the approved time. IA practitioners seek to protect and defend information and information systems by ensuring confidentiality, integrity, authentication, availability, and non-repudiation. These objectives are applicable whether the information is in storage, processing, or transit, and whether threatened by an attack. Answer: B is incorrect. ISSE is a set of processes and solutions used during all phases of a system's life cycle to meet the system's information protection needs.

**NEW QUESTION: 59**

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: (SHOW ANSWER)**

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.

**NEW QUESTION: 60**
Which of the following tiers addresses risks from an information system perspective?
**A.** Tier 0
**B.** Tier 3
**C.** Tier 2
**D.** Tier 1
**Answer: (SHOW ANSWER)**
The information system level is the tier 3. It addresses risks from an information system perspective, and is guided by the risk decisions at tiers 1 and 2. Risk decisions at tiers 1 and 2 impact the ultimate selection and deployment of requisite safeguards. This also has an impact on the countermeasures at the information system level. The RMF primarily operates at tier3 but it can also have interactions at tiers 1 and 2. Answer A is incorrect. It is an invalid Tier description. Answer D is incorrect. The Organization Level is the Tier 1, and it addresses risks from an organizational perspective. Answer C is incorrect. The mission and business process level is the Tier 2, and it addresses risks from the mission and business process perspective.

**NEW QUESTION: 61**
Which of the following security related areas are used to protect the confidentiality, integrity, and availability of federal information systems and information processed by those systems?
**A.** Personnel security
**B.** Access control
**C.** Configuration management
**D.** Media protection
**E.** Risk assessment
**Answer: A,B,C,D,E (LEAVE A REPLY)**
Explanation/Reference:
Explanation: The minimum security requirements cover seventeen security related areas to protect the confidentiality, integrity, and availability of federal information systems and information processed by those systems. They are as follows: Access control Awareness and training Audit and accountability Certification, accreditation, and security assessment Configuration management Contingency planning Identification and authentication Incident response Maintenance Media protection Physical and environmental protection Planning Personnel security Risk assessment Systems and services acquisition System and communications protection System and information integrity

**NEW QUESTION: 62**
Which of the following is a patch management utility that scans one or more computers on a network and alerts a user if any important Microsoft security patches are missing and also provides links that enable those missing patches to be downloaded and installed?
**A.** MABS
**B.** ASNB
**C.** MBSA
**D.** IDMS
**Answer: C (LEAVE A REPLY)**
Microsoft Baseline Security Analyzer (MBSA) is a tool that includes a graphical and command line interface that can perform local or remote scans of Windows systems. It runs on computers running Windows 2000, Windows XP, or Windows Server 2003 operating system. MBSA scans for common security misconfigurations in Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, Internet Information Server (IIS) 4.0 and above, SQL Server 7.0 and 2000, and Office 2000 and 2002. It also scans for missing hot fixes in several Microsoft products, such as Windows 2000, Windows XP, SQL Server etc. Answer B, D, and A are incorrect. These are invalid options.

**NEW QUESTION: 63**
SIMULATION
Fill in the blank with an appropriate phrase The is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity.
**Answer:**
Biba model
Explanation/Reference:
Explanation: 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.

**NEW QUESTION: 64**

Which of the following features of SIEM products is used in analysis for identifying potential problems and reviewing all available data that are associated with the problems?

**A.** Security knowledge base

**B.** Graphical user interface

**C.** Asset information storage and correlation

**D.** Incident tracking and reporting

**Answer: B (LEAVE A REPLY)**

SIEM product has a graphical user interface (GUI) which is used in analysis for identifying potential problems and reviewing all available data that are associated with the problems. A graphical user interface (GUI) is a type of user interface that allows people to interact with programs in more ways than typing commands on computers. The term came into existence because the first interactive user interfaces to computers were not graphical; they were text- and-keyboard oriented and usually consisted of commands a user had to remember and computer responses that were infamously brief. A GUI offers graphical icons, and visual indicators, as opposed to text-based interfaces, typed command labels or text navigation to fully represent the information and actions available to a user. The actions are usually performed through direct manipulation of the graphical elements.

**NEW QUESTION: 65**

Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?

**A.** Single Loss Expectancy (SLE)

**B.** Annualized Rate of Occurrence (ARO)

**C.** Safeguard

**D.** Exposure Factor (EF)

**Answer: B (LEAVE A REPLY)**

Explanation/Reference:

Explanation: The Annualized Rate of Occurrence (ARO) is a number that represents the estimated frequency at which a threat is expected to occur. It is calculated based upon the probability of the event occurring and the number of employees that could make that event occur. AnswerD is incorrect. The Exposure Factor (EF) represents the % of assets loss caused by a threat. The EF is required to calculate the Single Loss Expectancy (SLE). Answer: A is incorrect. The Single Loss Expectancy (SLE) is the value in dollars that is assigned to a single event. SLE = Asset Value ($) X Exposure Factor (EF) Answer: C is incorrect. Safeguard acts as a countermeasure for reducing the risk associated with a specific threat or a group of threats.

**NEW QUESTION: 66**

Which of the following requires all general support systems and major applications to be fully certified and accredited before these systems and applications are put into production? Each correct answer represents a part of the solution. Choose all that apply.

**A.** NIST

**B.** Office of Management and Budget (OMB)
**C.** FIPS
**D.** FISMA
**Answer: B,D (LEAVE A REPLY)**
Explanation/Reference:
Explanation: FISMA and Office of Management and Budget (OMB) require all general support systems and major applications to be fully certified and accredited before they are put into production. General support systems and major applications are also referred to as information systems and are required to be reaccredited every three years. AnswerA 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. Answer: C is incorrect. The Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States federal government for use by all non-military government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community (ANSI, IEEE, ISO, etc.). Some FIPS standards were originally developed by the U.S. government. For instance, standards for encoding data (e.g., country codes), but more significantly some encryption standards, such as the Data Encryption Standard (FIPS 46-3) and the Advanced Encryption Standard (FIPS 197). In 1994, NOAA (Noaa) began broadcasting coded signals called FIPS (Federal Information Processing System) codes along with their standard weather broadcasts from local stations. These codes identify the type of emergency and the specific geographic area (such as a county) affected by the emergency.

**NEW QUESTION: 67**
Which of the following areas of information system, as separated by Information Assurance Framework, is a collection of local computing devices, regardless of physical location, that are interconnected via local area networks (LANs) and governed by a single security policy?
**A.** Local Computing Environments
**B.** Networks and Infrastructures
**C.** Supporting Infrastructures
**D.** Enclave Boundaries
**Answer: (SHOW ANSWER)**
Explanation/Reference:
Explanation: The areas of information system, as separated by Information Assurance Framework, are as follows: Local Computing Environments: This area includes servers, client workstations, operating system, and applications. Enclave Boundaries: This area consists of collection of local computing devices, regardless of physical location, that are interconnected via local area networks (LANs) and governed by a single security policy. Networks and

Infrastructures: This area provides the network connectivity between enclaves. It includes operational area networks (OANs), metropolitan area networks (MANs), and campus area networks (CANs). Supporting Infrastructures: This area provides security services for networks, client workstations, Web servers, operating systems, applications, files, and single-use infrastructure machines

**NEW QUESTION: 68**
Which of the following are the basic characteristics of declarative security? Each correct answer represents a complete solution. Choose all that apply.
**A.** It is a container-managed security.
**B.** It has a runtime environment.
**C.** All security constraints are stated in the configuration files.
**D.** The security policies are applied at the deployment time.
**Answer: (SHOW ANSWER)**
Explanation/Reference:
Explanation: The following are the basic characteristics of declarative security: In declarative security, programming is not required. All security constraints are stated in the configuration files. It is a container- managed security. The application server manages the enforcing process of security constraints. It has a runtime environment. The security policies for runtime environment are represented by the deployment descriptor. It can support different environments, such as development, testing, and production. AnswerD is incorrect. It is the characteristic of programmatic security.

**NEW QUESTION: 69**
Which of the following scanning techniques helps to ensure that the standard software configuration is currently with the latest security patches and software, and helps to locate uncontrolled or unauthorized software?
**A.** Port Scanning
**B.** Discovery Scanning
**C.** Server Scanning
**D.** Workstation Scanning
**Answer: (SHOW ANSWER)**
Workstation scanning provides help to ensure that the standard software configuration exists with the most recent security patches and software. It helps to locate uncontrolled or unauthorized software. A full workstation vulnerability scan of the standard corporate desktop configuration must be implemented on a regularly basis. Answer B is incorrect. The discovery scanning technique is used to gather adequate information regarding each network device to identify what type of device it is, its operating system, and if it is running any externally vulnerable services, like Web services, FTP, or email. Answer C is incorrect. A full server vulnerability scan helps to determine if the server OS has been configured to the corporate standards and identify if applications have been updated with the latest security patches and software versions. Answer A

is incorrect. Port scanning technique describes the process of sending a data packet to a port to gather information about the state of the port.

**NEW QUESTION: 70**
Which of the following security design patterns provides an alternative by requiring that a user's authentication credentials be verified by the database before providing access to that user's data?
**A.** Secure assertion
**B.** Authenticated session
**C.** Password propagation
**D.** Account lockout
**Answer: (SHOW ANSWER)**
Explanation/Reference:
Explanation: Password propagation provides an alternative by requiring that a user's authentication credentials be verified by the database before providing access to that user's data.
Answer: D is incorrect.
Account lockout implements a limit on the incorrect password attempts to protect an account from automated password-guessing attacks. Answer: B is incorrect. Authenticated session allows a user to access more than one access-restricted Web page without re-authenticating every page. It also integrates user authentication into the basic session model. Answer: A is incorrect. Secure assertion distributes application-specific sanity checks throughout the system.

**NEW QUESTION: 71**
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 (LEAVE A REPLY)**
Explanation/Reference:
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. Management may develop a contingency plan if the risk does occur. Acceptance response to a risk event is a strategy that can be used for risks that pose either threats or opportunities. Acceptance response can be of two types:

Passive acceptance: It is a strategy in which no plans are made to try or avoid or mitigate the risk. Active acceptance: Such responses include developing contingency reserves to deal with risks, in case they occur. Acceptance is the only response for both threats and opportunities. AnswerB is incorrect.
Mitigation aims to lower the probability and/or impact of the risk event. AnswerC is incorrect. Transference transfers the ownership of the risk event to a third party, usually through a contractual agreement. AnswerD is incorrect. Enhance is a risk response that tries to increase the probability and/or impact of the positive risk event.

**NEW QUESTION: 72**
Which of the following is a standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system?
**A.** FITSAF
**B.** FIPS
**C.** TCSEC
**D.** SSAA
**Answer: C (LEAVE A REPLY)**
Explanation/Reference:
Explanation: Trusted Computer System Evaluation Criteria (TCSEC) is a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. TCSEC was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information. It was replaced with the development of the Common Criteria international standard originally published in 2005. The TCSEC, frequently referred to as the Orange Book, is the centerpiece of the DoD Rainbow Series publications. AnswerD is incorrect. System Security Authorization Agreement (SSAA) is an information security document used in the United States Department of Defense (DoD) to describe and accredit networks and systems. The SSAA is part of the Department of Defense Information Technology Security Certification and Accreditation Process, or DITSCAP (superseded by DIACAP). The DoD instruction (issues in December 1997, that describes DITSCAP and provides an outline for the SSAA document is DODI 5200.40. The DITSCAP application manual (DoD 8510.1- M), published in July 2000, provides additional details. Answer: A is incorrect. FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. It provides an approach for federal agencies. It determines how federal agencies are meeting existing policy and establish goals. The main advantage of FITSAF is that it addresses the requirements of Office of Management and Budget (OMB). It also addresses the guidelines provided by the National Institute of Standards and Technology (NIsT). Answer: B is incorrect. The Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States federal government for use by all non-military government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community (ANSI, IEEE, ISO, etc.). Some FIPS

standards were originally developed by the U.S. government. For instance, standards for encoding data (e.g., country codes), but more significantly some encryption standards, such as the Data Encryption Standard (FIPS 46-
3) and the Advanced Encryption Standard (FIPS 197). In 1994, NOAA (Noaa) began broadcasting coded signals called FIPS (Federal Information Processing System) codes along with their standard weather broadcasts from local stations. These codes identify the type of emergency and the specific geographic area (such as a county) affected by the emergency.

**NEW QUESTION: 73**
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 (LEAVE A REPLY)**
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.

**NEW QUESTION: 74**
Which of the following are the phases of the Certification and Accreditation (C&A) process? Each correct answer represents a complete solution. Choose two.
**A.** Continuous Monitoring
**B.** Auditing
**C.** Detection
**D.** Initiation
**Answer: A,D (LEAVE A REPLY)**

Explanation/Reference:
Explanation: The Certification and Accreditation (C&A) process consists of four distinct phases:
1.Initiation
2.Security Certification 3.Security Accreditation 4.Continuous Monitoring The C&A activities can be applied to an information system at appropriate phases in the system development life cycle by selectively tailoring the various tasks and subtasks. AnswerB and C are incorrect. Auditing and detection are not phases of the Certification and Accreditation process.

**NEW QUESTION: 75**
Which of the following phases of the DITSCAP C&A process is used to define the C&A level of effort, to identify the main C&A roles and responsibilities, and to create an agreement on the method for implementing the security requirements?
**A.** Phase 1
**B.** Phase 4
**C.** Phase 2
**D.** Phase 3
**Answer: A (LEAVE A REPLY)**
The Phase 1 of the DITSCAP C&A process 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. Answer C is incorrect. The Phase 2 of the DITSCAP C&A process is known as Verification. Answer D is incorrect. The Phase 3 of the DITSCAP C&A process is known as Validation. Answer B is incorrect. The Phase 4 of the DITSCAP C&A process is known as Post Accreditation.

**NEW QUESTION: 76**
Which of the following statements about a host-based intrusion prevention system (HIPS) are true? Each correct answer represents a complete solution. Choose two.
**A.** It can detect events scattered over the network.
**B.** It is a technique that allows multiple computers to share one or more IP addresses.
**C.** It can handle encrypted and unencrypted traffic equally.
**D.** It cannot detect events scattered over the network.
**Answer: (SHOW ANSWER)**
Explanation/Reference:
Explanation: A host-based intrusion prevention system (HIPS) is an application usually employed on a single computer. It complements traditional finger- print-based and heuristic antivirus detection methods, since it does not need continuous updates to stay ahead of new malware. When a malicious code needs to modify the system or other software residing on the machine, a HIPS system will notice some of the resulting changes and prevent the action by default or notify the user for permission. It can handle encrypted and unencrypted traffic equally and cannot detect events scattered over the network. AnswerB is incorrect. Network address translation (NAT) is a technique that allows multiple computers to share one or more IP addresses. NAT is configured

at the server between a private network and the Internet. It allows the computers in a private network to share a global, ISP assigned address. NAT modifies the headers of packets traversing the server. For packets outbound to the Internet, it translates the source addresses from private to public, whereas for packets inbound from the Internet, it translates the destination addresses from public to private. AnswerA is incorrect. Network intrusion prevention system (NIPS) is a hardware/software platform that is designed to analyze, detect, and report on security related events. NIPS is designed to inspect traffic and based on its configuration or security policy, it can drop malicious traffic.
NIPS is able to detect events scattered over the network and can react.



**NEW QUESTION: 77**
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 (LEAVE A REPLY)**
Explanation/Reference:
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.

**NEW QUESTION: 78**

Which of the following configuration management system processes keeps track of the changes so that the latest acceptable configuration specifications are readily available?

**A.** Configuration Control

**B.** Configuration Status and Accounting

**C.** Configuration Verification and Audit

**D.** Configuration Identification

**Answer: B (LEAVE A REPLY)**

The configuration status accounting procedure is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time. It supports the functional and physical attributes of software at various points in time, and performs systematic control of accounting to the identified attributes for the purpose of maintaining software integrity and traceability throughout the software development life cycle. The configuration status and accounting process keeps track of the changes so that the latest acceptable configuration specifications are readily available. Answer C is incorrect. The verification and audit processes seek to establish a high level of confidence in how well the Configuration Management activity is working. 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 D 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.

**NEW QUESTION: 79**

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 (LEAVE A REPLY)**

Explanation/Reference:

Explanation: The concept of authentication establishes the users' identity and ensures that the users are who they say they are. AnswerB 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.

**NEW QUESTION: 80**
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 (LEAVE A REPLY)**
Explanation/Reference:
Explanation: Security Test and Evaluation (ST&E) occurs in Phase 3 of the DITSCAP C&A process.
AnswerD 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 AnswerA 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 AnswerB 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

**NEW QUESTION: 81**
Security controls are safeguards or countermeasures to avoid, counteract, or minimize security risks.
Which of the following are types of security controls? Each correct answer represents a complete solution.
Choose all that apply.
**A.** Common controls
**B.** Hybrid controls
**C.** Storage controls

**D.** System-specific controls

**Answer: A,B,D (LEAVE A REPLY)**

Explanation/Reference:

Explanation: Security controls are safeguards or countermeasures to avoid, counteract, or minimize security risks. The following are the types of security controls for information systems, that can be employed by an organization: 1.System-specific controls: These types of security controls provide security capability for a particular information system only. 2.Common controls: These types of security controls provide security capability for multiple information systems. 3.Hybrid controls: These types of security controls have features of both system-specific and common controls. AnswerC is incorrect. It is an invalid control.

**NEW QUESTION: 82**

You work as a Security Manager for Tech Perfect Inc. The company has a Windows based network. It is required to determine compatibility of the systems with custom applications. Which of the following techniques will you use to accomplish the task?

**A.** Safe software storage

**B.** Antivirus management

**C.** Backup control

**D.** Software testing

**Answer: (SHOW ANSWER)**

Explanation/Reference:

Explanation: In order to accomplish the task, you should use the software testing technique. By using this technique you can determine compatibility of systems with custom applications or you can identify other unforeseen interactions. You can also use the software testing technique while you are upgrading software. AnswerB is incorrect. You can use the antivirus management to save the systems from viruses, unexpected software interactions, and the subversion of security controls. Answer: A is incorrect. You can use the safe software storage technique to ensure that the software and backup copies have not been modified without authorization. Answer: C is incorrect. You can use the backup control to perform back up of software and data.

**NEW QUESTION: 83**

Which of the following techniques is used to identify attacks originating from a botnet?

**A.** Passive OS fingerprinting

**B.** Recipient filtering

**C.** IFilter

**D.** BPF-based filter

**Answer: A (LEAVE A REPLY)**

Explanation/Reference:

Explanation: Passive OS fingerprinting can identify attacks originating from a botnet. Network Administrators can configure the firewall to take action on a botnet attack by using information obtained from passive OS fingerprinting. Passive OS fingerprinting (POSFP) allows the sensor to

determine the operating system used by the hosts. The sensor examines the traffic flow between two hosts and then stores the operating system of those two hosts along with their IP addresses. In order to determine the type of operating system, the sensor analyzes TCP SYN and SYN ACK packets that are traveled on the network. The sensor computes the attack relevance rating to determine the relevancy of victim attack using the target host OS. After it, the sensor modifies the alert's risk rating or filters the alert for the attack.
Passive OS fingerprinting is also used to improve the alert output by reporting some information, such as victim OS, relevancy to the victim in the alert, and source of the OS identification.
AnswerD is incorrect. A BPF-based filter is used to limit the number of packets seen by tcpdump; this renders the output more usable on networks with a high volume of traffic. Answer: B is incorrect. Recipient filtering is used to block messages on the basis of whom they are sent to. Answer: C is incorrect. IFilters are used to extract contents from files that are crawled. IFilters also remove application-specific formatting before the content of a document is indexed by the search engine.

**NEW QUESTION: 84**
Numerous information security standards promote good security practices and define frameworks or systems to structure the analysis and design for managing information security controls. Which of the following are the international information security standards? Each correct answer represents a complete solution. Choose all that apply.
**A.** AU audit and accountability
**B.** Human resources security
**C.** Organization of information security
**D.** Risk assessment and treatment
**Answer: B,C,D (LEAVE A REPLY)**
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 businesscritical 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.

**NEW QUESTION: 85**
Which of the following processes describes the elements such as quantity, quality, coverage, timelines, and availability, and categorizes the different functions that the system will need to perform in order to gather the documented mission/business needs?
**A.** Human factors
**B.** Functional requirements
**C.** Performance requirements
**D.** Operational scenarios
**E.** Explanation:
The functional requirements categorize the different functions that the system will need to perform in order to gather the documented mission/business needs. The functional requirements describe the elements such as quantity, quality, coverage, timelines, and availability.
**Answer: (SHOW ANSWER)**
is incorrect. The performance requirements comprise of speed, throughput, accuracy, humidity tolerances, mechanical stresses such as vibrations or noises. Answer A is incorrect. Human factor consists of factors, which affect the operation of the system or component, such as design space, eye movement, or ergonomics. Answer D is incorrect. The operational scenarios provide assistance to the system designers and form the basis of major events in the acquisition phases, such as testing the products for system integration. The customer classifies and defines the operational scenarios, which indicate the range of anticipated uses of system products.

**NEW QUESTION: 86**
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: A,C,D,E (LEAVE A REPLY)**
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.

**NEW QUESTION: 87**
Which of the following are the common roles with regard to data in an information classification program? Each correct answer represents a complete solution. Choose all that apply.

**A.** Editor
**B.** Custodian
**C.** Owner
**D.** User
**E.** Security auditor
**Answer: B,C,D,E (LEAVE A REPLY)**
The following are the common roles with regard to data in an information classification program: Owner Custodian User Security auditor The following are the responsibilities of the owner with regard to data in an information classification program: Determining what level of classification the information requires. Reviewing the classification assignments at regular time intervals and making changes as the business needs change. Delegating the responsibility of the data protection duties to the custodian. The following are the responsibilities of the custodian with regard to data in an information classification program: Running regular backups and routinely testing the validity of the backup data Performing data restoration from the backups when necessary Controlling access, adding and removing privileges for individual users The users must comply with the requirements laid out in policies and procedures. They must also exercise due care. A security auditor examines an organization's security procedures and mechanisms.

**NEW QUESTION: 88**
Which of the following persons in an organization is responsible for rejecting or accepting the residual risk for a system?
**A.** Information Systems Security Officer (ISSO)
**B.** Designated Approving Authority (DAA)
**C.** System Owner
**D.** Chief Information Security Officer (CISO)
**Answer: B (LEAVE A REPLY)**
The authorizing official is the senior manager responsible for approving the working of the information system. He is responsible for the risks of operating the information system within a known environment through the security accreditation phase. In many organizations, the authorizing official is also referred as approving/accrediting authority (DAA) or the Principal Approving Authority (PAA). Answer C is incorrect. The system owner has the responsibility of informing the key officials within the organization of the requirements for a security C&A of the information system. He makes the resources available, and provides the relevant documents to support the process. Answer A is incorrect. 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. Answer D is incorrect. The CISO has the

responsibility of carrying out the CIO's FISMA responsibilities. He manages the information security program functions.

**NEW QUESTION: 89**
Which of the following processes will you involve to perform the active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures?
**A.** Penetration testing
**B.** Baselining
**C.** Risk analysis
**D.** Compliance checking
**Answer: (SHOW ANSWER)**
Explanation/Reference:
Explanation: A penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered. It is a component of a full security audit. AnswerC 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 D is incorrect. Compliance checking performs the reviews for safeguards and controls to verify whether the entity is complying with particular procedures, rules or not. It includes the inspection of operational systems to guarantee that hardware and software controls have been correctly implemented and maintained. Compliance checking covers the activities such as penetration testing and vulnerability assessments. Compliance checking must be performed by skilled persons, or by an automated software package. Answer: B is incorrect. Baselining is a method for analyzing the performance of computer networks. The method is marked by comparing the current performance to a historical metric, or "baseline". For example, if a user measured the performance of a network switch over a period of time, he could use that performance figure as a comparative baseline if he made a configuration change to the switch.

**NEW QUESTION: 90**

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 (LEAVE A REPLY)**

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.

**NEW QUESTION: 91**

There are seven risks responses that a project manager can choose from. Which risk response is appropriate for both positive and negative risk events?

**A.** Acceptance

**B.** Transference

**C.** Sharing

**D.** Mitigation

**Answer: A (LEAVE A REPLY)**

Only acceptance is appropriate for both positive and negative risk events. Often sharing is used for low probability and low impact risk events regardless of the positive or negative effects the risk event may bring the project. 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. Management may develop a contingency plan if the risk does occur. Acceptance response to a risk event is a strategy that can be used for risks that pose either threats or opportunities. Acceptance response can be of two types: Passive acceptance: It is a strategy in which no plans are made to try or avoid or mitigate the risk. Active acceptance: Such responses include developing contingency reserves to deal with risks, in case they occur. Acceptance is the only response for both threats and opportunities. Answer C is incorrect. Sharing is a positive risk response that shares an opportunity for all parties involved in the risk event. Answer B is incorrect. Transference is a negative risk event that transfers the risk ownership to a third party, such as vendor, through a contractual relationship. Answer D is incorrect. Mitigation is a negative risk event that seeks to lower the probability and/or impact of a risk event.

**NEW QUESTION: 92**
Which of the following policies can explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations?
**A.** Informative
**B.** Advisory
**C.** Selective
**D.** Regulatory
**Answer: A (LEAVE A REPLY)**
An informative policy informs employees about certain topics. It is not an enforceable policy, but rather one to teach individuals about specific issues relevant to the company. The informative policy can explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations. Answer D is incorrect. A regulatory policy ensures that an organization follows the standards set by specific industry regulations. This type of policy is very detailed and specific to a type of industry. The regulatory policy is used in financial institutions, health care facilities, public utilities, and other government-regulated industries, e.g., TRAI. Answer B is incorrect. An advisory policy strongly advises employees regarding which types of behaviors and activities should and should not take place within the organization. It also outlines possible ramifications if employees do not comply with the established behaviors and activities. The advisory policy can be used to describe how to handle medical information, handle financial transactions, and process confidential information. Answer C is incorrect. It is not a valid type of policy.

**NEW QUESTION: 93**
In digital rights management, the level of robustness depends on the various types of tools and attacks to which they must be resistant or immune. Which of the following types of tools are expensive, require skill, and are not easily available?
**A.** Hand tools
**B.** Widely available tools
**C.** Specialized tools
**D.** Professional tools
**Answer: D (LEAVE A REPLY)**
Explanation/Reference:

Explanation: The tools used in DRM to define the level of robustness are as follows: 1.Widely available tools: These tools are easy to use and are available to everyone. For example, screw-drivers and file editors. 2.Specialized tools: These tools require skill and are available at reasonable prices. For example, debuggers, decompilers, and memory scanners. 3.Professional tools: These tools are expensive, require skill, and are not easily available. For example, logic analyzers, circuit emulators, and chip disassembly systems.

**NEW QUESTION: 94**
Copyright holders, content providers, and manufacturers use digital rights management (DRM) in order to limit usage of digital media and devices. Which of the following security challenges does DRM include?
Each correct answer represents a complete solution. Choose all that apply.
**A.** OTA provisioning
**B.** Access control
**C.** Key hiding
**D.** Device fingerprinting
**Answer: A,C,D (LEAVE A REPLY)**
Explanation/Reference:
Explanation: The security challenges for DRM are as follows: Key hiding: It prevents tampering attacks that target the secret keys. In the key hiding process, secret keys are used for authentication, encryption, and node-locking. Device fingerprinting: It prevents fraud and provides secure authentication. Device fingerprinting includes the summary of hardware and software characteristics in order to uniquely identify a device. OTA provisioning: It provides end-to-end encryption or other secure ways for delivery of copyrighted software to mobile devices. AnswerB is incorrect. Access control is not a security challenge for DRM.

**NEW QUESTION: 95**
NIST SP 800-53A defines three types of interview depending on the level of assessment conducted. Which of the following NIST SP 800-53A interviews consists of informal and ad hoc interviews?
**A.** Comprehensive
**B.** Significant
**C.** Abbreviated
**D.** Substantial
**Answer: C (LEAVE A REPLY)**
Explanation/Reference:
Explanation: Abbreviated interview consists of informal and ad hoc interviews. AnswerD is incorrect.
Substantial interview consists of informal and structured interviews. AnswerA is incorrect.
Comprehensive interview consists of formal and structured interviews. Answer: B is incorrect.
There is no such type of interview in NIST SP 800-53A.

**NEW QUESTION: 96**
Which of the following elements of the BCP process emphasizes on creating the scope and the additional elements required to define the parameters of the plan?
**A.** Business continuity plan development
**B.** Plan approval and implementation
**C.** Business impact analysis
**D.** Scope and plan initiation
**Answer: D (LEAVE A REPLY)**
The scope and plan initiation process in BCP symbolizes the beginning of the BCP process. It emphasizes on creating the scope and the additional elements required to define the parameters of the plan. The scope and plan initiation phase embodies a check of the company's operations and support services. The scope activities include creating a detailed account of the work required, listing the resources to be used, and defining the management practices to be employed. Answer C is incorrect. The business impact assessment is a method used to facilitate business units to understand the impact of a disruptive event. This phase includes the execution of a vulnerability assessment. This process makes out the mission-critical areas and business processes that are important for the survival of business. It is similar to the risk assessment process. The function of a business impact assessment process is to create a document, which is used to help and understand what impact a disruptive event would have on the business. Answer A is incorrect. The business continuity plan development refers to the utilization of the information collected in the Business Impact Analysis (BIA) for the creation of the recovery strategy plan to support the critical business functions. The information gathered from the BIA is mapped out to make a strategy for creating a continuity plan. The business continuity plan development process includes the areas of plan implementation, plan testing, and ongoing plan maintenance. This phase also consists of defining and documenting the continuity strategy. Answer B is incorrect. The plan approval and implementation process involves creating enterprise-wide awareness of the plan, getting the final senior management signoff, and implementing a maintenance procedure for updating the plan as required.

**NEW QUESTION: 97**
Shoulder surfing is a type of in-person attack in which the attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard of an employee's computer while he is typing in his password at any access point such as a terminal/Web site. Which of the following is violated in a shoulder surfing attack?
**A.** Integrity
**B.** Availability
**C.** Confidentiality
**D.** Authenticity
**Answer: C (LEAVE A REPLY)**

Confidentiality is violated in a shoulder surfing attack. The CIA triad provides the following three tenets for which security practices are measured: Confidentiality: It is the property of preventing disclosure of information to unauthorized individuals or systems. Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Integrity: It means that data cannot be modified without authorization. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on. Availability: It means that data must be available at every time when it is needed. Answer D is incorrect. Authenticity is not a tenet of the CIA triad.

**NEW QUESTION: 98**
Which of the following refers to a process that is used for implementing information security?
**A.** Classic information security model
**B.** Five Pillars model
**C.** Certification and Accreditation (C&A)
**D.** Information Assurance (IA)
**Answer: (SHOW ANSWER)**
Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The C&A process is used extensively in the U.S. Federal Government. Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. Answer D is incorrect. Information Assurance (IA) is the practice of managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. While focused dominantly on information in digital form, the full range of IA encompasses not only digital but also analog or physical form. Information assurance as a field has grown from the practice of information security, which in turn grew out of practices and procedures of computer security. Answer A is incorrect. The classic information security model is used in the practice of Information Assurance (IA) to define assurance requirements. The classic information security model, also called the CIA Triad, addresses three attributes of information and information

systems, confidentiality, integrity, and availability. This C-I-A model is extremely useful for teaching introductory and basic concepts of information security and assurance; the initials are an easy mnemonic to remember, and when properly understood, can prompt systems designers and users to address the most pressing aspects of assurance. Answer B is incorrect. The Five Pillars model is used in the practice of Information Assurance (IA) to define assurance requirements. It was promulgated by the U.S. Department of Defense (DoD) in a variety of publications, beginning with the National Information Assurance Glossary, Committee on National Security Systems Instruction CNSSI-4009. Here is the definition from that publication: "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." The Five Pillars model is sometimes criticized because authentication and non-repudiation are not attributes of information or systems; rather, they are procedures or methods useful to assure the integrity and authenticity of information, and to protect the confidentiality of the same.

**NEW QUESTION: 99**
You work as a Network Auditor for Net Perfect Inc. The company has a Windows-based network. While auditing the company's network, you are facing problems in searching the faults and other entities that belong to it. Which of the following risks may occur due to the existence of these problems?
**A.** Residual risk
**B.** Secondary risk
**C.** Detection risk
**D.** Inherent risk
**Answer: C (LEAVE A REPLY)**
Explanation/Reference:
Explanation: Detection risks are the risks that an auditor will not be able to find what they are looking to detect. Hence, it becomes tedious to report negative results when material conditions (faults) actually exist.
Detection risk includes two types of risk: Sampling risk: This risk occurs when an auditor falsely accepts or erroneously rejects an audit sample. Nonsampling risk: This risk occurs when an auditor fails to detect a condition because of not applying the appropriate procedure or using procedures inconsistent with the audit objectives (detection faults). Answer: A is incorrect. Residual risk is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures). The formula to calculate residual risk is (inherent risk) x (control risk) where inherent risk is (threats vulnerability). In the economic context, residual means "the quantity left over at the end of a process; a remainder". Answer: D is incorrect. Inherent risk, in auditing, is the risk that the account or section being audited is materially misstated without considering internal controls due to error or fraud. The assessment of inherent risk depends on the professional judgment of the auditor, and it is

done after assessing the business environment of the entity being audited. Answer: B is incorrect. A secondary risk is a risk that arises as a straight consequence of implementing a risk response. The secondary risk is an outcome of dealing with the original risk. Secondary risks are not as rigorous or important as primary risks, but can turn out to be so if not estimated and planned properly.

**NEW QUESTION: 100**
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: (SHOW ANSWER)**
Explanation/Reference:
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. AnswerC is incorrect. Such material would cause "damage" or be "prejudicial" to national security if publicly available.
AnswerB 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.

**NEW QUESTION: 101**
You work as a Security Manager for Tech Perfect Inc. You want to save all the data from the SQL injection attack, which can read sensitive data from the database and modify database data using some commands, such as Insert, Update, and Delete. Which of the following tasks will you perform? Each correct answer represents a complete solution. Choose three.
**A.** Apply maximum number of database permissions.
**B.** Use an encapsulated library for accessing databases.
**C.** Create parameterized stored procedures.
**D.** Create parameterized queries by using bound and typed parameters.
**Answer: (SHOW ANSWER)**
Explanation/Reference:

Explanation: The methods of mitigating SQL injection attacks are as follows: 1.Create parameterized queries by using bound and typed parameters. 2.Create parameterized stored procedures. 3.Use a encapsulated library in order to access databases. 4.Minimize database permissions. AnswerA is incorrect. In order to save all the data from the SQL injection attack, you should minimize database permissions.

**NEW QUESTION: 102**
Which of the following security models focuses on data confidentiality and controlled access to classified information?
**A.** Clark-Wilson model
**B.** Biba model
**C.** Take-Grant model
**D.** Bell-La Padula model
**Answer: (SHOW ANSWER)**
The Bell-La Padula Model is a state machine model used for enforcing access control in government and military applications. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g.,"Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public"). The Bell-La Padula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity. Answer B is incorrect. 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. Answer A is incorrect. The Clark-Wilson model provides a foundation for specifying and analyzing an integrity policy for a computing system. The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. The model's enforcement and certification rules define data items and processes that provide the basis for an integrity policy. The core of the model is based on the notion of a transaction. Answer C is incorrect. 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.

**NEW QUESTION: 103**

Stella works as a system engineer for BlueWell Inc. She wants to identify the performance thresholds of each build. Which of the following tests will help Stella to achieve her task?

**A.** Reliability test

**B.** Performance test

**C.** Regression test

**D.** Functional test

**Answer: B (LEAVE A REPLY)**

The various types of internal tests performed on builds are as follows: Regression tests: It is also known as the verification testing. These tests are developed to confirm that capabilities in earlier builds continue to work correctly in the subsequent builds. Functional test: These tests emphasizes on verifying that the build meets its functional and data requirements and correctly generates each expected display and report. Performance tests: These tests are used to identify the performance thresholds of each build. Reliability tests: These tests are used to identify the reliability thresholds of each build.

**NEW QUESTION: 104**

Which of the following is an example of over-the-air (OTA) provisioning in digital rights management?

**A.** Use of shared secrets to initiate or rebuild trust.

**B.** Use of software to meet the deployment goals.

**C.** Use of concealment to avoid tampering attacks.

**D.** Use of device properties for unique identification.

**Answer: A (LEAVE A REPLY)**

Explanation/Reference:

Explanation: Over- the- air provisioning is a mechanism to deploy MIDlet suites over a network. It is a method of distributing MIDlet suites. MIDlet suite providers install their MIDlet suites on Web servers and provide a hypertext link for downloading. A user can use this link to download the MIDlet suite either through the Internet microbrowser or through WAP on his device. Over-the-air provisioning is required for end-to-end encryption or other security purposes in order to deliver copyrighted software to a mobile device. For example, use of shared secrets to initiate or rebuild trust. Answer: D and C are incorrect. The use of device properties for unique identification and the use of concealment to avoid tampering attacks are the security challenges in digital rights management (DRM). Answer: B is incorrect. The use of software and hardware to meet the deployment goals is a distracter.

**NEW QUESTION: 105**

In which of the following processes are experienced personnel and software tools used to investigate, resolve, and handle process deviation, malformed data, infrastructure, or connectivity issues?

**A.** Risk Management

**B.** Exception management

**C.** Configuration Management
**D.** Change Management
**E.** Explanation:
Exception management is a process in which experienced personnel and software tools are used to investigate, resolve, and handle process deviation, malformed data, infrastructure or connectivity issues. It increases the efficiency of business processes and contributes in the progress of business.
**Answer: B (LEAVE A REPLY)**
is incorrect. Configuration Management (CM) is an Information Technology Infrastructure Library (ITIL) IT Service Management (ITSM) process. It tracks all of the individual Configuration Items (CI) in an IT system, which may be as simple as a single server, or as complex as the entire IT department. In large organizations a configuration manager may be appointed to oversee and manage the CM process. Answer A is incorrect. Risk Management is used to identify, assess, and control risks. It includes analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats. Risk Management is part of Service Design and the owner of the Risk Management is the Risk Manager. Risks are addressed within several processes in ITIL V3; however, there is no dedicated Risk Management process. ITIL V3 calls for "coordinated risk assessment exercises", so at IT Process Maps we decided to assign clear responsibilities for managing risks. Answer D is incorrect. Change Management is used to ensure that standardized methods and procedures are used for efficient handling of all changes. A change is "an event that results in a new status of one or more configuration items (CI's)" approved by management, cost effective, enhances business process changes (fixes) - with a minimum risk to IT infrastructure. The main aims of Change Management are as follows: Minimal disruption of services Reduction in back-out activities Economic utilization of resources involved in the change

**NEW QUESTION: 106**
Which of the following US Acts emphasized a "risk-based policy for cost-effective security" and makes mandatory for agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget?
**A.** Federal Information Security Management Act of 2002 (FISMA)
**B.** The Electronic Communications Privacy Act of 1986 (ECPA)
**C.** The Equal Credit Opportunity Act (ECOA)
**D.** The Fair Credit Reporting Act (FCRA)
**Answer: A (LEAVE A REPLY)**
Explanation/Reference:
The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. 3541, et seq.) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899). The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal

agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA has brought attention within the federal government to cybersecurity and explicitly emphasized a "risk-based policy for cost-effective security".
FISMA requires agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget (OMB).
OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act. Answer C is incorrect. The Equal Credit Opportunity Act (ECOA) is a United States law (codified at 15 U S C 1691 et seq), enacted in 1974, that makes it unlawful for any creditor to discriminate against any applicant, with respect to any aspect of a credit transaction, on the basis of race, color, religion, national origin, sex, marital status, or age; to the fact that all or part of the applicant's income derives from a public assistance program; or to the fact that the applicant has in good faith exercised any right under the Consumer Credit Protection Act. The law applies to any person who, in the ordinary course of business, regularly participates in a credit decision, including banks, retailers, bankcard companies, finance companies, and credit unions. Answer B is incorrect. The Electronic Communications Privacy Act of 1986 (ECPA Pub. L 99-508, Oct 21, 1986,
100 Stat. 1848, 18 U.S.C. 2510) was enacted by the United States Congress to extend government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer.
Specifically, ECPA was an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of
1968 (the Wiretap Statute), which was primarily designed to prevent unauthorized government access to private electronic communications. The ECPA also added new provisions prohibiting access to stored electronic communications, i.e., the Stored Communications Act,18 U.S.C. 2701-2712. AnswerD is incorrect. The Fair Credit Reporting Act (FCRA) is an American federal law (codified at 15 U.S.C. 1681 et seq.) that regulates the collection, dissemination, and use of consumer information, including consumer credit information. Along with the Fair Debt Collection Practices Act (FDCPA), it forms the base of consumer credit rights in the United States. It was originally passed in 1970, and is enforced by the US Federal Trade Commission.

**NEW QUESTION: 107**
You work as a project manager for BlueWell Inc. You are working on a project and the management wants a rapid and cost-effective means for establishing priorities for planning risk responses in your project. Which risk management process can satisfy management's objective for your project?
**A.** Qualitative risk analysis
**B.** Historical information
**C.** Rolling wave planning
**D.** Quantitative analysis
**Answer: (SHOW ANSWER)**
Qualitative risk analysis is the best answer as it is a fast and low-cost approach to analyze the risk impact and its effect. It can promote certain risks onto risk response planning. Qualitative Risk Analysis uses the likelihood and impact of the identified risks in a fast and cost-effective manner. Qualitative Risk Analysis establishes a basis for a focused quantitative analysis or Risk Response Plan by evaluating the precedence of risks with a concern to impact on the project's scope, cost, schedule, and quality objectives. The qualitative risk analysis is conducted at any point in a project life cycle. The primary goal of qualitative risk analysis is to determine proportion 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.

**NEW QUESTION: 108**
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.
**E.** Explanation:
Risk management is an ongoing project activity. It should be an agenda item at every project status meeting.

**Answer: D,E (LEAVE A REPLY)**
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.

**NEW QUESTION: 109**
SIMULATION
Fill in the blank with an appropriate phrase. models address specifications, requirements, design, verification and validation, and maintenance activities.
**Answer:**
Life cycle
Explanation/Reference:
Explanation: A life cycle model helps to provide an insight into the development process and emphasizes on the relationships among the different activities in this process. This model describes a structured approach to the development and adjustment process involved in producing and maintaining systems. The life cycle model addresses specifications, design, requirements, verification and validation, and maintenance activities.

**NEW QUESTION: 110**
Which of the following are the initial steps required to perform a risk analysis process? Each correct answer represents a part of the solution. Choose three.
**A.** Valuations of the critical assets in hard costs.
**B.** Evaluate potential threats to the assets.
**C.** Estimate the potential losses to assets by determining their value.
**D.** Establish the threats likelihood and regularity.
**Answer: (SHOW ANSWER)**
Explanation/Reference:
Explanation: The main steps of performing risk analysis are as follows: Estimate the potential losses to the assets by determining their value. Evaluate the potential threats to the assets. Establish the threats probability and regularity. Answer A is incorrect. Valuations of the critical assets in hard costs is one of the final steps taken after performing the risk analysis.

**NEW QUESTION: 111**
Which of the following steps of the LeGrand Vulnerability-Oriented Risk Management method determines the necessary compliance offered by risk management practices and assessment of risk levels?
**A.** Assessment, monitoring, and assurance
**B.** Vulnerability management
**C.** Risk assessment
**D.** Adherence to security standards and policies for development and deployment

**Answer: A (LEAVE A REPLY)**
Explanation/Reference:
Explanation: Assessment, monitoring, and assurance determines the necessary compliance that are offered by risk management practices and assessment of risk levels.

**NEW QUESTION: 112**
Numerous information security standards promote good security practices and define frameworks or systems to structure the analysis and design for managing information security controls. Which of the following are the U.S. Federal Government information security standards? Each correct answer represents a complete solution. Choose all that apply.
**A.** IR Incident Response
**B.** Information systems acquisition, development, and maintenance
**C.** SA System and Services Acquisition
**D.** CA Certification, Accreditation, and Security Assessments
**Answer: A,C,D (LEAVE A REPLY)**
Following are the various U.S. Federal Government information security standards: AC Access Control AT Awareness and Training AU Audit and Accountability CA Certification, Accreditation, and Security Assessments CM Configuration Management CP Contingency Planning IA Identification and Authentication IR Incident Response MA Maintenance MP Media Protection PE Physical and Environmental Protection PL Planning PS Personnel Security RA Risk Assessment SA System and Services Acquisition SC System and Communications Protection SI System and Information Integrity Answer B is incorrect. Information systems acquisition, development, and maintenance is an International information security standard.

**NEW QUESTION: 113**
Which of the following are included in Technical Controls? Each correct answer represents a complete solution. Choose all that apply.
**A.** Identification and authentication methods
**B.** Configuration of the infrastructure
**C.** Password and resource management
**D.** Implementing and maintaining access control mechanisms
**E.** Security devices
**F.** Conducting security-awareness training
**Answer: (SHOW ANSWER)**
Technical Controls are also known as Logical Controls. These controls include the following: Implementing and maintaining access control mechanisms Password and resource management Identification and authentication methods Security devices Configuration of the infrastructure Answer F is incorrect. It is a part of Administrative Controls.

**NEW QUESTION: 114**

Which of the following refers to the ability to ensure that the data is not modified or tampered with?

**A.** Integrity

**B.** Availability

**C.** Non-repudiation

**D.** Confidentiality

**Answer: A (LEAVE A REPLY)**

Explanation/Reference:

Explanation: Integrity refers to the ability to ensure that the data is not modified or tampered with. Integrity means that data cannot be modified without authorization. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a Web site, when someone is able to cast a very large number of votes in an online poll, and so on. AnswerD is incorrect. Confidentiality is the property of preventing disclosure of information to unauthorized individuals or systems. Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. AnswerB is incorrect. Availability means that data must be available whenever it is needed. AnswerC is incorrect. Non-repudiation is the concept of ensuring that a party in a dispute cannot refuse to acknowledge, or refute the validity of a statement or contract. As a service, it provides proof of the integrity and origin of data. Although this concept can be applied to any transmission, including television and radio, by far the most common application is in the verification and trust of signatures.

**NEW QUESTION: 115**

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

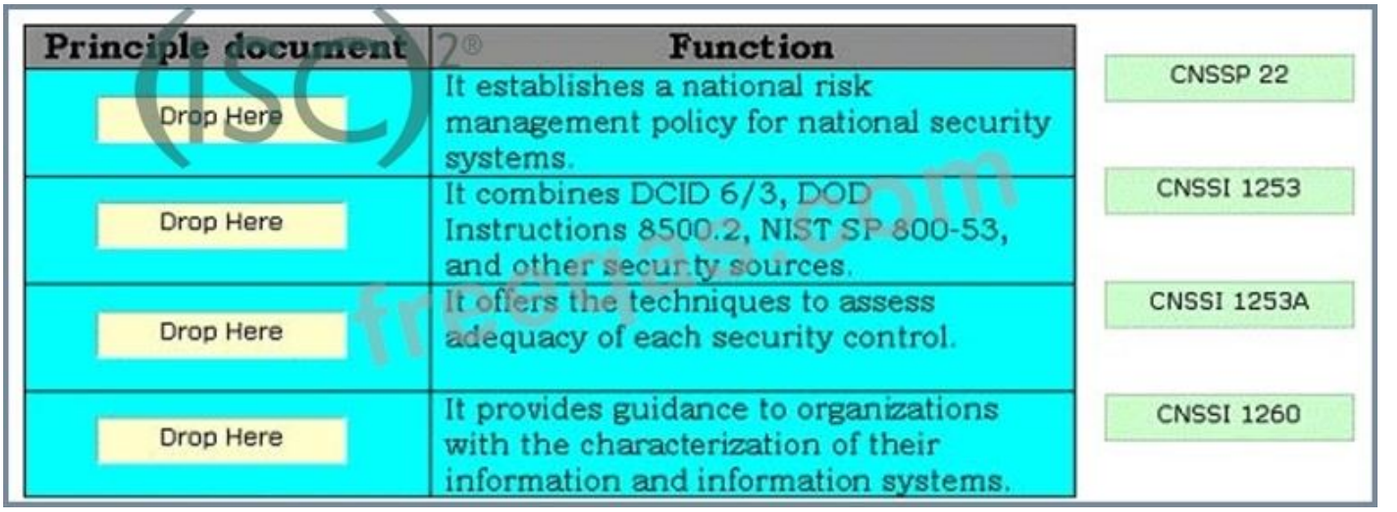
**Answer: B (LEAVE A REPLY)**

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

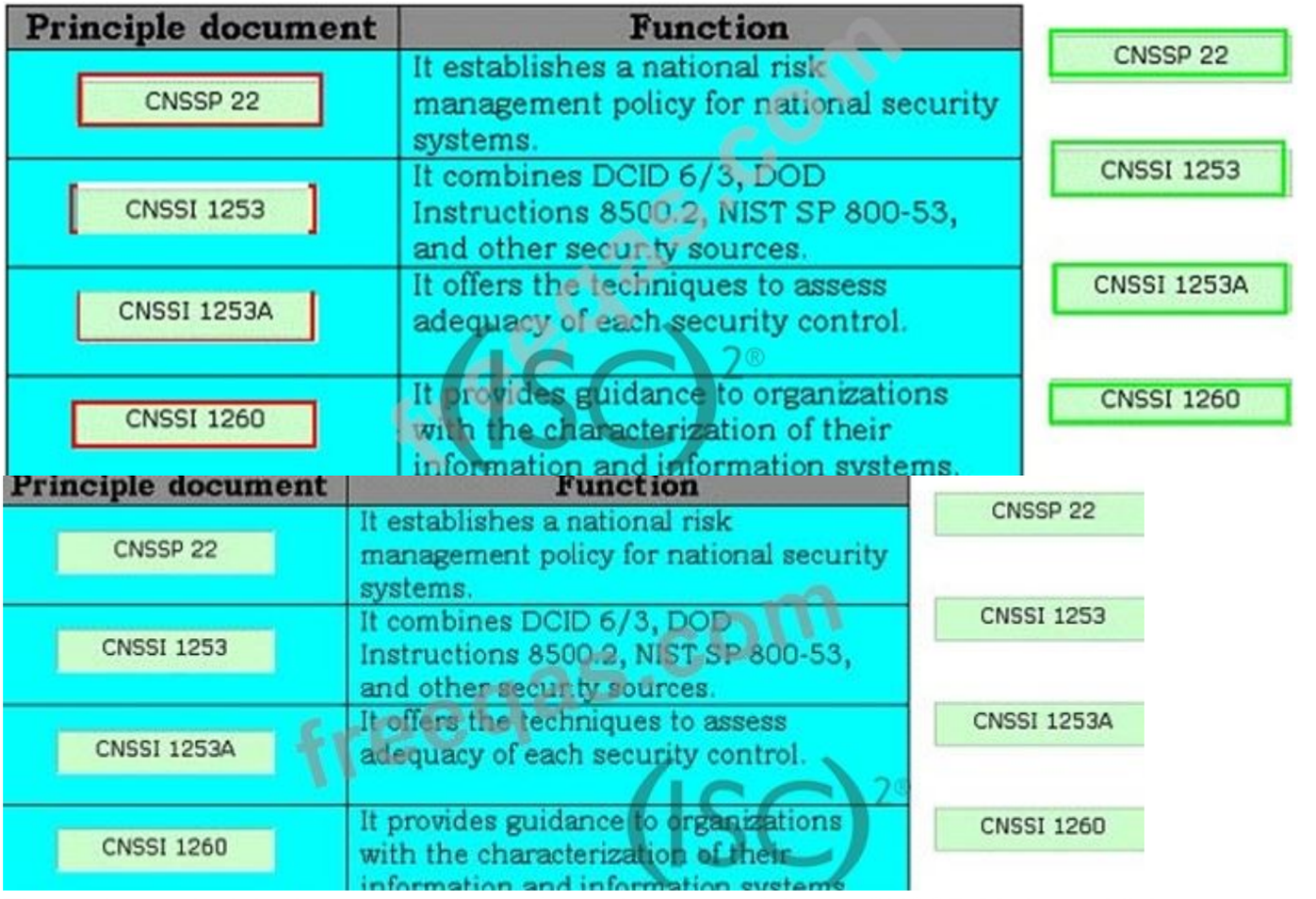
specialist to ensure that the software meets the requirement for which it was made. Answer A is incorrect. Integration testing is a logical extension of unit testing. It is performed to identify the problems that occur when two or more units are combined into a component. During integration testing, 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.

**NEW QUESTION: 116**
Which of the following security objectives are defined for information and information systems by the FISMA? Each correct answer represents a part of the solution. Choose all that apply.
**A.** Authenticity
**B.** Availability
**C.** Integrity
**D.** Confidentiality
**Answer: B,C,D (LEAVE A REPLY)**
Explanation/Reference:
Explanation: FISMA defines the following three security objectives for information and information systems:
Confidentiality: It means that the data should only be accessible to authorized users. Access includes printing, displaying, and other such forms of disclosure, including simply revealing the existence of an object. Integrity: It means that only authorized users are able to modify data. Modification admits changing, changing the status, deleting, and creating. Availability: It means that the data should only be available to authorized users. AnswerA is incorrect. Authenticity is not defined by the FISMA as one of the security objectives for information and information systems.

**NEW QUESTION: 117**
DRAG DROP
Drag and drop the appropriate principle documents in front of their respective functions.




**Answer:**




The various principle documents of transformation are as follows: CNSSP 22: It establishes a national risk management policy for national security systems. CNSSI 1199: It creates the technique in which the national security community classifies the information and information systems with regard to confidentiality, integrity, and availability. CNSSI 1253: It combines DCID 6/3, DOD Instructions 8500.2, NIST SP 800-53, and other security sources into a single cohesive repository of security controls. CNSSI 1253 A.

It offers the techniques to assess adequacy of each security control. CNSSI 1260: It provides guidance to organizations with the characterization of their information and information systems.

NIST 800-37, Revision 1: It defines the certification and accreditation (C & A) process. The NIST 800-37, Revision 1 is a combination of DNI, DoD, and NIST.

**NEW QUESTION: 118**
You work as a security engineer for BlueWell Inc. You want to use some techniques and procedures to verify the effectiveness of security controls in Federal Information System. Which of the following NIST documents will guide you?
**A.** NIST Special Publication 800-53
**B.** NIST Special Publication 800-59
**C.** NIST Special Publication 800-53A
**D.** NIST Special Publication 800-37
**Answer: C (LEAVE A REPLY)**
Explanation/Reference:
Explanation: NIST has developed a suite of documents for conducting Certification & Accreditation (C&A).
These documents are as follows: 1.NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems. 2.NIST Special Publication 800-53:
This document provides a guideline for security controls for Federal Information Systems. 3.NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System. 4.NIST Special Publication 800-59: This document provides a guideline for identifying an information system as a National Security System. 5.NIST Special Publication 800-60: This document is a guide for mapping types of information and information systems to security objectives and risk levels.

**NEW QUESTION: 119**
Which of the following US Acts emphasized a "risk-based policy for cost-effective security" and makes mandatory for agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget?
**A.** Federal Information Security Management Act of 2002 (FISMA)
**B.** The Electronic Communications Privacy Act of 1986 (ECPA)
**C.** The Equal Credit Opportunity Act (ECOA)
**D.** The Fair Credit Reporting Act (FCRA)
**Answer: (SHOW ANSWER)**
The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. 3541, et seq.) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899). The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the

agency, including those provided or managed by another agency, contractor, or other source. FISMA has brought attention within the federal government to cybersecurity and explicitly emphasized a "risk-based policy for cost-effective security". FISMA requires agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget (OMB). OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act. Answer C is incorrect. The Equal Credit Opportunity Act (ECOA) is a United States law (codified at 15 U.S.C. 1691 et seq.), enacted in 1974, that makes it unlawful for any creditor to discriminate against any applicant, with respect to any aspect of a credit transaction, on the basis of race, color, religion, national origin, sex, marital status, or age; to the fact that all or part of the applicant's income derives from a public assistance program; or to the fact that the applicant has in good faith exercised any right under the Consumer Credit Protection Act. The law applies to any person who, in the ordinary course of business, regularly participates in a credit decision, including banks, retailers, bankcard companies, finance companies, and credit unions. Answer B is incorrect. The Electronic Communications Privacy Act of 1986 (ECPA Pub.L. 99-508, Oct. 21, 1986, 100 Stat. 1848, 18 U.S.C. 2510) was enacted by the United States Congress to extend government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer. Specifically, ECPA was an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Wiretap Statute), which was primarily designed to prevent unauthorized government access to private electronic communications. The ECPA also added new provisions prohibiting access to stored electronic communications, i.e., the Stored Communications Act,18 U.S.C. 2701-2712. Answer D is incorrect. The Fair Credit Reporting Act (FCRA) is an American federal law (codified at 15 U.S.C. 1681 et seq.) that regulates the collection, dissemination, and use of consumer information, including consumer credit information. Along with the Fair Debt Collection Practices Act (FDCPA), it forms the base of consumer credit rights in the United States. It was originally passed in 1970, and is enforced by the US Federal Trade Commission.

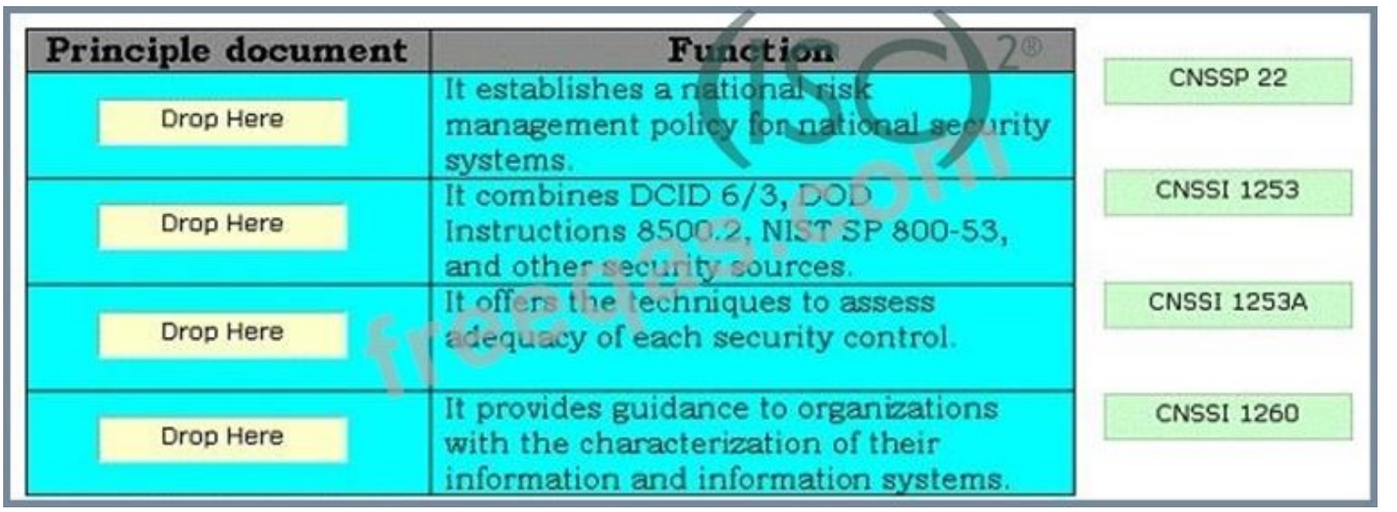
**NEW QUESTION: 120**
The Web resource collection is a security constraint element summarized in the Java Servlet Specification v2.4. Which of the following elements does it include? Each correct answer represents a complete solution. Choose two.
**A.** HTTP methods
**B.** Role names
**C.** Transport guarantees
**D.** URL patterns
**Answer: (SHOW ANSWER)**
Explanation/Reference:
Explanation: Web resource collection is a set of URL patterns and HTTP operations that define all resources required to be protected. It is a security constraint element summarized in the Java Servlet Specification v2.4. The Web resource collection includes the following elements: URL

patterns HTTP methods AnswerB is incorrect. An authorization constraint includes role names. Answer: C is incorrect. A user data constraint includes transport guarantees.

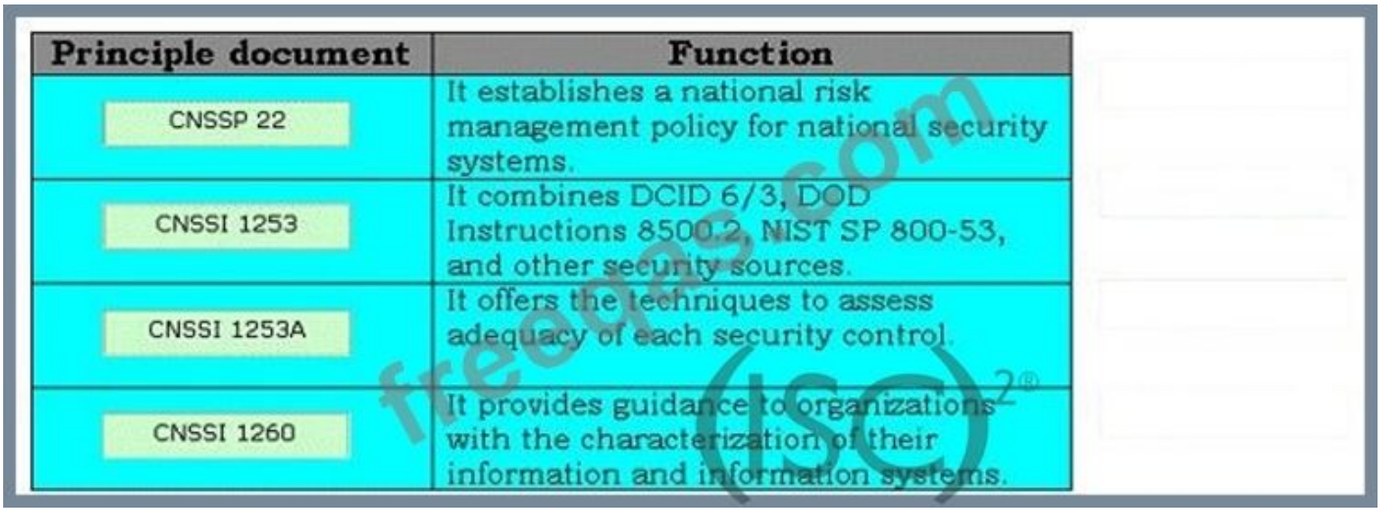
**NEW QUESTION: 121**
Which of the following DITSCAP C&A phases takes place between the signing of the initial version of the SSAA and the formal accreditation of the system?
**A.** Phase 4
**B.** Phase 3
**C.** Phase 1
**D.** Phase 2
**Answer: D (LEAVE A REPLY)**
The Phase 2 of DITSCAP C&A is known 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. Answer C, B, and A are incorrect. These phases do not take place between the signing of the initial version of the SSAA and the formal accreditation of the system.



**NEW QUESTION: 122**
DRAG DROP
Drag and drop the appropriate principle documents in front of their respective functions.
Select and Place:




**Answer:**




Explanation/Reference:

The various principle documents of transformation are as follows: CNSSP 22: It establishes a national risk management policy for national security systems. CNSSI 1199: It creates the technique in which the national security community classifies the information and information systems with regard to confidentiality, integrity, and availability. CNSSI 1253: It combines DCID 6/3, DOD Instructions 8500.2, NIST SP 800-53, and other security sources into a single cohesive repository of security controls. CNSSI

1253 A It offers the techniques to assess adequacy of each security control. CNSSI 1260: It provides guidance to organizations with the characterization of their information and information systems. NIST 800-

37, Revision 1: It defines the certification and accreditation (C & A) process. The NIST 800-37, Revision 1 is a combination of DNI, DoD, and NIST.

**NEW QUESTION: 123**

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: A,B,C (LEAVE A REPLY)**

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.