ISC.CSSLP.v2022-05-21.q194

Exam Code:	CSSLP
Exam Name:	Certified Secure Software Lifecycle Professional Practice Test
Certification Provider:	ISC
Free Question Number:	194
Version:	v2022-05-21
# of views:	3333
# of Questions views:	1940
https://www.exam-tests.com/CSSLP-exam/ISC.CSSLP.v2022-05-21.q194.html	

NEW QUESTION: 1
DRAG DROP
Drag and drop the correct DoD Policy Series at their appropriate places.
Select and Place:
Answer:
Explanation/Reference:
Explanation: The various DoD policy series are as follows:

NEW QUESTION: 2
Which of the following DoD directives defines DITSCAP as the standard C&A process for the Department of Defense?
A. DoD 8910.1
B. DoD 5200.22-M
C. DoD 8000.1
D. DoD 5200.40
Answer: D (LEAVE A REPLY)
DITSCAP stands for DoD Information Technology Security Certification and Accreditation Process. The DoD Directive 5200.40 (DoD Information Technology Security Certification and Accreditation Process) established the DITSCAP as the standard C&A process for the Department of Defense. The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk. DIACAP replaced the former process, known as DITSCAP, in 2006. Answer B is incorrect. This DoD Directive is known as National Industrial Security Program Operating Manual. Answer C is incorrect. This DoD Directive is known as Defense Information Management (IM) Program. Answer A is incorrect. This DoD Directive is known as Management and Control of Information Requirements.

NEW QUESTION: 3
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: 4
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)
Explanation/Reference:
Explanation: 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. AnswerE is incorrect. This feature is not required for these tools.

NEW QUESTION: 5
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)

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. Answer A 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: 6
You are the project manager for your organization. You are preparing for the quantitative risk analysis.
Mark, a project team member, wants to know why you need to do quantitative risk analysis when you just completed qualitative risk analysis. Which one of the following statements best defines what quantitative risk analysis is?
A. Quantitative risk analysis is the process of prioritizing risks for further analysis or action by assessing and combining their probability of occurrence and impact.
B. Quantitative risk analysis is the review of the risk events with the high probability and the highest impact on the project objectives.
C. Quantitative risk analysis is the planning and quantification of risk responses based on probability and impact of each risk event.
D. Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation: Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives. It is performed on risk that have been prioritized through the qualitative risk analysis process. AnswerA is incorrect. This is actually the definition of qualitative risk analysis. Answer:
B is incorrect. While somewhat true, this statement does not completely define the quantitative risk analysis process. AnswerC is incorrect. This is not a valid statement about the quantitative risk analysis process. Risk response planning is a separate project management process.

NEW QUESTION: 7
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)

Explanation/Reference:
Explanation: 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: 8
Maria has been recently appointed as a Network Administrator in Gentech Inc. She has been tasked to perform network security testing to find out the vulnerabilities and shortcomings of the present network infrastructure. Which of the following testing approaches will she apply to accomplish this task?
A. Gray-box testing
B. White-box testing
C. Black-box testing
D. Unit testing
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: Maria is new for this organization and she does not have any idea regarding the present infrastructure. Therefore, black box testing is best suited for her. Blackbox testing is a technique in which the testing team has no knowledge about the infrastructure of the organization. The testers must first determine the location and extent of the systems before commencing their analysis. This testing technique is costly and time consuming. AnswerB is incorrect. White box testing, also known as Clear box or Glass box testing, takes into account the internal mechanism of a system or application. The connotations of
"Clear box" and "Glass box" indicate that a tester has full visibility of the internal workings of the system. It uses knowledge of the internal structure of an application. It is applicable at the unit, integration, and system levels of the software testing process. It consists of the following testing methods: Control flow- based testing Create a graph from source code. Describe the flow of control through the control flow graph. Design test cases to cover certain elements of the graph. Data flow-based testing Test connections between variable definitions. Check variation of the control flow graph. Set DEF (n) contains variables that are defined at node n. Set USE (n) are variables that are read. AnswerA is incorrect. Graybox testing is a combination of whitebox testing and blackbox testing. In graybox testing, the test engineer is equipped with the knowledge of system and designs test cases or test data based on system knowledge. The security tester typically performs graybox testing to find vulnerabilities in software and network system. Answer D is incorrect. Unit testing is a type of testing in which each independent unit of an application is tested separately. During unit testing, a developer takes the smallest unit of an application, isolates it from the rest of the application code, and tests it to determine whether it works as expected. Unit testing is performed before integrating these independent units into modules. The most common approach to unit testing requires drivers and stubs to be written. Drivers and stubs are programs. A driver simulates a calling unit, and a stub simulates a called unit.

NEW QUESTION: 9
You are the project manager of the NNN project for your company. You and the project team are working together to plan the risk responses for the project. You feel that the team has successfully completed the risk response planning and now you must initiate what risk process it is. Which of the following risk processes is repeated after the plan risk responses to determine if the overall project risk has been satisfactorily decreased?
A. Quantitative risk analysis
B. Risk identification
C. Risk response implementation
D. Qualitative risk analysis
Answer: A (LEAVE A REPLY)
The quantitative risk analysis process is repeated after the plan risk responses to determine if the overall project risk has been satisfactorily decreased. Answer D is incorrect. Qualitative risk analysis is not repeated after the plan risk response process. Answer B is incorrect. Risk identification is an ongoing process that happens throughout the project. Answer C is incorrect. Risk response implementation is not a project management process.

NEW QUESTION: 10
Digital rights management (DRM) consists of compliance and robustness rules. Which of the following features does the robustness rule have? Each correct answer represents a complete solution. Choose three.
A. It specifies the various levels of robustness that are needed for asset security.
B. It specifies minimum techniques for asset security.
C. It specifies the behaviors of the DRM implementation and applications accessing the implementation.
D. It contains assets, such as device key, content key, algorithm, and profiling data.
Answer: A,B,D (LEAVE A REPLY)
Explanation/Reference:
Explanation: The DRM (digital rights management) technology includes the following rules:
1.Compliance rule: This rule specifies the behaviors of the DRM implementation, and applications that are accessing the implementation. The compliance rule specifies the following elements: Definition of specific license rights Device requirements Revocation of license path or penalties when the implementation is not robust enough or noncompliant 2.Robustness rule: This rule has the following features: It specifies the various levels of robustness that are needed for asset security. It contains assets, such as device key, content key, algorithm, and profiling data. It specifies minimum techniques for asset security.

NEW QUESTION: 11
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)
Explanation/Reference:
Explanation: 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 AnswerC is incorrect. Determining what level of classification the information requires is the responsibility of the owner.

NEW QUESTION: 12
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: 13
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: (SHOW ANSWER)
Explanation/Reference:
Explanation: 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.

NEW QUESTION: 14
Which of the following methods is a means of ensuring that system changes are approved before being implemented, only the proposed and approved changes are implemented, and the implementation is complete and accurate?
A. Configuration control
B. Documentation control
C. Configuration identification
D. Configuration auditing
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: Documentation control is a method of ensuring that system changes should be agreed upon before being implemented, only the proposed and approved changes are implemented, and the implementation is complete and accurate. Documentation control is

involved in the strict events for proposing, monitoring, and approving system changes and their implementation. It helps the change process by supporting the person who synchronizes the analytical task, approves system changes, reviews the implementation of changes, and oversees other tasks such as documenting the controls.
AnswerD is incorrect. Configuration auditing is the quality assurance element of configuration management. It is occupied in the process of periodic checks to establish the consistency and completeness of accounting information and to validate that all configuration management policies are being followed. Configuration audits are broken into functional and physical configuration audits. They occur either at delivery or at the moment of effecting the change. A functional configuration audit ensures that functional and performance attributes of a configuration item are achieved, while a physical configuration audit ensures that a configuration item is installed in accordance with the requirements of its detailed design documentation. AnswerA is incorrect. Configuration control is a procedure of the Configuration management. Configuration control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them. It supports the change of the functional and physical attributes of software at various points in time, and performs systematic control of changes to the identified attributes. Answer C is incorrect. Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/ or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined. Baselining an attribute forces formal configuration change control processes to be effected in the event that these attributes are changed.

NEW QUESTION: 15
In which of the following deployment models of cloud is the cloud infrastructure administered by the organizations or a third party? Each correct answer represents a complete solution. Choose two.
A. Private cloud
B. Public cloud
C. Hybrid cloud
D. Community cloud
Answer: A,D (LEAVE A REPLY)
Explanation/Reference:
Explanation: In private cloud, the cloud infrastructure is operated exclusively for an organization. The private cloud infrastructure is administered by the organization or a third party, and exists on premise and off premise. In community cloud, the cloud infrastructure is shared by a number of organizations and supports a particular community. The community cloud infrastructure is administered by the organizations or a third party and exists on premise or off premise. AnswerB is incorrect. In public cloud, the cloud infrastructure is administered by an organization that sells cloud services. AnswerC is incorrect. In hybrid cloud, the cloud infrastructure is administered by both, i.e., an organization and a third party.

NEW QUESTION: 16
You work as a system engineer for BlueWell Inc. You want to verify that the build meets its data requirements, and correctly generates each expected display and report. Which of the following tests will help you to perform the above task?
A. Performance test
B. Functional test
C. Reliability test
D. Regression test
Answer: (SHOW ANSWER)
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: 17
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: 18
A service provider guarantees for end-to-end network traffic performance to a customer. Which of the following types of agreement is this?
A. SLA
B. VPN
C. NDA
D. LA
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: This is a type of service-level agreement. A service-level agreement (SLA) is a negotiated agreement between two parties where one is the customer and the other is the service provider. It records a common understanding about services, priorities, responsibilities, guarantees, and warranties. Each area of service scope should have the 'level of service' defined. The SLA may specify the levels of availability, serviceability, performance, operation, or other attributes of the service, such as billing. AnswerC is incorrect. Non-disclosure agreements (NDAs) are often used to protect the confidentiality of an invention as it is being evaluated by potential

licensees. AnswerD is incorrect. License agreements (LA) describe the rights and responsibilities of a party related to the use and exploitation of intellectual property. Answer:
B is incorrect. There is no such type of agreement as VPN.

NEW QUESTION: 19
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: (SHOW ANSWER)
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: 20
ISO 27003 is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Which of the following elements does this standard contain? Each correct answer represents a complete solution. Choose all that apply.
A. Inter-Organization Co-operation
B. Information Security Risk Treatment
C. CSFs (Critical success factors)
D. ystem requirements for certification bodies Managements
E. Terms and Definitions
F. Guidance on process approach
Answer: (SHOW ANSWER)
ISO 27003 is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is entitled as "Information Technology - Security techniques - Information security management system implementation guidance". The ISO 27003 standard provides guidelines for implementing an ISMS (Information Security Management System). It mainly focuses upon the PDCA method along with establishing, implementing, reviewing, and improving the ISMS itself. The ISO 27003 standard contains the following elements: Introduction Scope Terms and Definitions CSFs

(Critical success factors) Guidance on process approach Guidance on using PDCA Guidance on Plan Processes Guidance on Do Processes Guidance on Check Processes Guidance on Act Processes Inter-Organization Co-operation Answer B is incorrect. This element is included in the ISO 27005 standard. Answer D is incorrect. This element is included in the ISO 27006 standard.

NEW QUESTION: 21
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: B (LEAVE A REPLY)
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. Answer A 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: 22
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: A (LEAVE A REPLY)
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. Answer C 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: 23
Security is a state of well-being of information and infrastructures in which the possibilities of successful yet undetected theft, tampering, and/or disruption of information and services are kept low or tolerable. Which of the following are the elements of security? Each correct answer represents a complete solution. Choose all that apply.
A. Integrity
B. Authenticity
C. Confidentiality
D. Availability
Answer: A,B,C,D (LEAVE A REPLY)
Explanation/Reference:
Explanation: The elements of security are as follows: 1.Confidentiality: It is the concealment of information or resources. 2.Authenticity: It is the identification and assurance of the origin of information. 3.Integrity: It refers to the trustworthiness of data or resources in terms of preventing improper and unauthorized changes. 4.Availability: It refers to the ability to use the information or resources as desired.

NEW QUESTION: 24
System Authorization is the risk management process. System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. What are the different phases of System Authorization Plan? Each correct answer represents a part of the solution. Choose all that apply.
A. Post-certification
B. Post-Authorization
C. Authorization
D. Pre-certification

E. Certification

Answer: B,C,D,E (LEAVE A REPLY)

Explanation/Reference:

Explanation: The creation of System Authorization Plan (SAP) is mandated by System Authorization.

System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. It consists of four phases: Phase 1 - Pre-certification Phase 2 - Certification Phase 3 - Authorization Phase 4 - Post-Authorization

NEW QUESTION: 25

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: B,C,D (LEAVE A REPLY)

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: 26

Della works as a security engineer for BlueWell Inc. She wants to establish configuration management and control procedures that will document proposed or actual changes to the information system. Which of the following phases of NIST SP 800-37 C&A methodology will define the above task?

A. Initiation

B. Security Certification

C. Continuous Monitoring

D. Security Accreditation

Answer: C (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: 27
The NIST ITL Cloud Research Team defines some primary and secondary technologies as the fundamental elements of cloud computing in its "Effectively and Securely Using the Cloud Computing Paradigm" presentation. Which of the following technologies are included in the primary technologies? Each correct answer represents a complete solution. Choose all that apply.
A. Web application framework
B. Free and open source software
C. SOA
D. Virtualization
E. Explanation:
The primary technologies defined by the NIST ITL Cloud Research Team in its "Effectively and Securely Using the Cloud Computing Paradigm" presentation are as follows: Virtualization Grid technology SOA (Service Oriented Architecture) Distributed computing Broadband network Browser as a platform Free and open source software
Answer: B,C,D,E (LEAVE A REPLY)
is incorrect.
It is defined as the secondary technology.

NEW QUESTION: 28
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: (SHOW ANSWER)
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: 29

FIPS 199 defines the three levels of potential impact on organizations: low, moderate, and high. Which of the following are the effects of loss of confidentiality, integrity, or availability in a high level potential impact?

A. The loss of confidentiality, integrity, or availability might result in a major damage to organizational assets.

B. The loss of confidentiality, integrity, or availability might result in severe damages like life threatening injuries or loss of life.

C. The loss of confidentiality, integrity, or availability might result in major financial losses.

D. The loss of confidentiality, integrity, or availability might cause severe degradation in or loss of mission capability to an extent.

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

The following are the effects of loss of confidentiality, integrity, or availability in a high level potential impact: It might cause a severe degradation in or loss of mission capability to an extent. It might result in a major damage to organizational assets. It might result in a major financial loss. It might result in severe harms such as serious life threatening injuries or loss of life.

NEW QUESTION: 30

Which of the following concepts represent the three fundamental principles of information security? Each correct answer represents a complete solution. Choose three.

A. Privacy

B. Availability

C. Integrity

D. Confidentiality

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation: The following concepts represent the three fundamental principles of information security:

1.Confidentiality 2.Integrity 3.Availability AnswerB is incorrect. Privacy, authentication, accountability, authorization and identification are also concepts related to information security, but they do not represent the fundamental principles of information security.

NEW QUESTION: 31

Which of the following is the most secure method of authentication?

A. Biometrics

B. Username and password

C. Anonymous

D. Smart card

Answer: A (LEAVE A REPLY)

Biometrics is a method of authentication that uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user. Nowadays, the usage of biometric devices such as hand scanners and retinal scanners is becoming more

common in the business environment. It is the most secure method of authentication. Answer B is incorrect. Username and password is the least secure method of authentication in comparison of smart card and biometrics authentication. Username and password can be intercepted. Answer D is incorrect. Smart card authentication is not as reliable as biometrics authentication. Answer C is incorrect. Anonymous authentication does not provide security as a user can log on to the system anonymously and he is not prompted for credentials.

NEW QUESTION: 32
Which of the following is a malicious exploit of a website, whereby unauthorized commands are transmitted from a user trusted by the website?
A. Cross-Site Scripting
B. Injection flaw
C. Side channel attack
D. Cross-Site Request Forgery
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
CSRF (Cross-Site Request Forgery) is a malicious exploit of a website, whereby unauthorized commands are transmitted from a user trusted by the website. It is also known as a one-click attack or session riding.
CSRF occurs when a user is tricked by an attacker into activating a request in order to perform some unauthorized action. It increases data loss and malicious code execution. AnswerA is incorrect. Cross- site scripting (XSS) is a type of computer security vulnerability typically found in web applications which enable malicious attackers to inject client-side script into web pages viewed by other users. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls, such as the same origin policy. Cross-site scripting carried out on websites were roughly 80% of all security vulnerabilities documented by Symantec as of 2007. Their impact may range from a petty nuisance to a significant security risk, depending on the sensitivity of the data handled by the vulnerable site, and the nature of any security mitigations implemented by the site owner. Answer: C is incorrect. A side channel attack is based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms (compare cryptanalysis). For example, timing

information, power consumption, electromagnetic leaks or even sound can provide an extra source of information which can be exploited to break the system. Many side- channel attacks require considerable technical knowledge of the internal operation of the system on which the cryptography is implemented. Answer: B is incorrect.
Injection flaws are the vulnerabilities where a foreign agent illegally uses a sub-system. They are the vulnerability holes that can be used to attack a database of Web applications. It is the most common technique of attacking a database. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing involuntary commands or changing data. Injection flaws include XSS (HTML Injection) and SQL Injection.

NEW QUESTION: 33
Which of the following terms refers to a mechanism which proves that the sender really sent a particular message?
A. Confidentiality
B. Non-repudiation
C. Authentication
D. Integrity
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: Non-repudiation is a mechanism which proves that the sender really sent a message. It provides an evidence of the identity of the senderand message integrity. It also prevents a person from denying the submission or delivery of the message and the integrity of its contents. AnswerC is incorrect.
Authentication is a process of verifying the identity of a person or network host. AnswerA is incorrect.
Confidentiality ensures that no one can read a message except the intended receiver. AnswerD is incorrect. Integrity assures the receiver that the received message has not been altered in any way from the original.

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)
Explanation/Reference:
Explanation: 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. AnswerC 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. AnswerA 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
In which of the following deployment models of cloud is the cloud infrastructure operated exclusively for an organization?
A. Public cloud
B. Community cloud
C. Private cloud
D. Hybrid cloud
Answer: C (LEAVE A REPLY)
In private cloud, the cloud infrastructure is operated exclusively for an organization.
The private cloud infrastructure is administered by the organization or a third party, and exists on premise and off premise.

NEW QUESTION: 36
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)
Explanation/Reference:
Explanation: 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). AnswerC 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. AnswerD is incorrect. The CISO has the responsibility of carrying out the CIO's FISMA responsibilities. He manages the information security program functions.

NEW QUESTION: 37
You are responsible for network and information security at a metropolitan police station. The most important concern is that unauthorized parties are not able to access data. What is this called?
A. Confidentiality
B. Availability
C. Integrity
D. Encryption
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation: The CIA (Confidentiality, Integrity, and Availability) triangle is concerned with three facets of security. Confidentiality is the concern that data be secure from unauthorized access. AnswerB and C are incorrect. The CIA (Confidentiality, Integrity, and Availability) triangle is concerned with three facets of security. Integrity is the concern that data not be altered without it being traceable. Availability is the concern that the data, while being secured, is readily accessible. AnswerD is incorrect. Confidentiality may be implemented with encryption but encryption is just a technique to obtain confidentiality.

NEW QUESTION: 38
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: 39

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: 40

Which of the following software review processes increases the software security by removing the common vulnerabilities, such as format string exploits, race conditions, memory leaks, and buffer overflows?

A. Management review

B. Code review

C. Peer review

D. Software audit review

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation: A code review is a systematic examination of computer source code, which searches and resolves issues occurred in the initial development phase. It increases the software security by removing common vulnerabilities, such as format string exploits, race conditions, memory leaks, and buffer overflows. A code review is performed in the following forms: Pair programming Informal walkthrough Formal inspection Answer: C is incorrect. A peer review is an examination process in which author and one or more colleagues examine a work product, such as document, code, etc., and evaluate technical content and quality. According to the Capability Maturity Model, peer review offers a systematic engineering practice in order to detect and resolve issues occurring in the software artifacts, and stops the leakage into field operations. Answer: A is incorrect. Management review is a management study into a project's status and allocation of resources. Answer: D is incorrect. In software audit review one or more auditors, who are not members of the software development organization, perform an independent examination of a software product, software process, or a set of software processes for assessing compliance with specifications, standards, contractual agreements, or other specifications.

NEW QUESTION: 41

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: (SHOW ANSWER)

The concept of authentication establishes the users' identity and ensures that the users are who they say they are. Answer B is incorrect. The concept of availability ensures the reliable and timely access to data or resources. Answer D is incorrect. The concept of integrity ensures that modifications are not made to data by unauthorized personnel or processes. Answer C is incorrect. The concept of accountability determines the actions and behaviors of a single individual within a system, and identifies that particular individual.

NEW QUESTION: 42

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.
Select and Place:
Answer:
Explanation/Reference:
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: 43
Which of the following ISO standards provides guidelines for accreditation of an organization that is concerned with certification and registration related to ISMS?
A. ISO 27006
B. ISO 27005
C. ISO 27003
D. ISO 27004
Answer: A (LEAVE A REPLY)
Explanation/Reference:
ISO 27006 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 - Requirements for bodies providing audit and certification of information security management systems". The ISO 27006 standard provides guidelines for accreditation of an organization which is concerned with certification and registration related to ISMS.
The ISO 27006 standard contains the following elements: Scope Normative references Terms and definitions Principles General requirements Structural requirements Resource requirements Information requirements Process requirements Management system requirements for certification bodies Information security risk communication Information security risk monitoring and review Annex A.
Defining the scope of process Annex B.
Asset valuation and impact assessment Annex C.
Examples of typical threats Annex D.
Vulnerabilities and vulnerability assessment methods Annex E.
Information security risk assessment (ISRA) approaches Answer: C is incorrect. The ISO 27003 standard provides guidelines for implementing an ISMS (Information Security Management System). Answer: D is incorrect. 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. Answer: B is incorrect. The ISO 27005 standard provides guidelines for information security risk management.

NEW QUESTION: 44
Which of the following characteristics are described by the DIAP Information Readiness Assessment function? Each correct answer represents a complete solution. Choose all that apply.
A. It provides for entry and storage of individual system data.
B. It performs vulnerability/threat analysis assessment.
C. It provides data needed to accurately assess IA readiness.
D. It identifies and generates IA requirements.
Answer: B,C,D (LEAVE A REPLY)
The characteristics of the DIAP Information Readiness Assessment function are as follows: It provides data needed to accurately assess IA readiness. It identifies and generates IA requirements. It performs vulnerability/threat analysis assessment. Answer A is incorrect. It is a function performed by the ASSET system.

NEW QUESTION: 45
Which of the following statements is true about residual risks?
A. It is the probabilistic risk after implementing all security measures.
B. It can be considered as an indicator of threats coupled with vulnerability.
C. It is a weakness or lack of safeguard that can be exploited by a threat.
D. It is the probabilistic risk before implementing all security measures.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation: The residual risk is the risk or danger of an action or an event, a method or a (technical) process that still conceives these dangers even if all theoretically possible safety measures would be applied. The formula to calculate residual risk is (inherent risk) x (control risk) where inherent risk is (threats vulnerability). Answer: B is incorrect. In information security, security risks are considered as an indicator of threats coupled with vulnerability. In other words, security risk is a probabilistic function of a given threat agent exercising a particular vulnerability and the impact of that risk on the organization.
Security risks can be mitigated by reviewing and taking responsible actions based on possible risks.
Answer C is incorrect. Vulnerability is a weakness or lack of safeguard that can be exploited by a threat,
thus causing harm to the information systems or networks. It can exist in hardware , operating systems, firmware, applications, and configuration files. Vulnerability has been variously defined in the current context as follows: 1.A security weakness in a Target of Evaluation due to failures in analysis, design, implementation, or operation and such. 2.Weakness in an information system or components (e.g. system security procedures, hardware design, or internal controls that could be

exploited to produce an information-related misfortune.) 3.The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the system, network, application, or protocol involved.

NEW QUESTION: 46
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: 47
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: (SHOW ANSWER)
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: 48
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: (SHOW ANSWER)
The confidentiality service of a cryptographic system ensures that information will not be disclosed to any unauthorized person on a local network.

NEW QUESTION: 49
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)
Explanation/Reference:
Explanation: Regression testing can be performed any time when a program needs to be modified either to add a feature or to fix an error. It is a process of repeating Unit testing and Integration testing whenever existing tests need to be performed again along with the new tests. Regression testing is performed to ensure that no existing errors reappear, and no new errors are introduced. AnswerD 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: 50
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: 51
Which of the following is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known, but by which a business can obtain an economic advantage over its competitors?
A. Copyright
B. Utility model
C. Trade secret
D. Cookie
E. Explanation:
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: C (LEAVE A REPLY)
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 B is incorrect. A utility model is an intellectual property right to protect inventions. Answer D is incorrect. A cookie is a small bit of text that accompanies requests and pages as they move between Web servers and browsers. It contains information that is read by a Web application, whenever a user visits a site. Cookies are stored in the memory or hard disk of client computers. A Web site stores information, such as user preferences and settings in a cookie. This information helps in providing customized services to users. There is absolutely no way a Web server can access any private information about a user or his computer through cookies, unless a user provides the information. A Web server cannot access cookies created by other Web servers.

NEW QUESTION: 52
The DoD 8500 policy series represents the Department's information assurance strategy. Which of the following objectives are defined by the DoD 8500 series? Each correct answer represents a complete solution. Choose all that apply.
A. Defending systems
B. Providing IA Certification and Accreditation
C. Providing command and control and situational awareness
D. Protecting information
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: The various objectives of the DoD 8500 series are as follows: Protecting information Defending systems Providing command and control and situational awareness Making sure that the information assurance is integrated into processes Increasing security awareness throughout the DoD's workforce

NEW QUESTION: 53
Which of the following processes provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and the security posture of a system or site?
A. NSA-IAM
B. NIACAP
C. ASSET
D. DITSCAP
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: NIACAP is a process, which provides a standard set of activities, general tasks, and a management structure to certify and accredit systems that maintain the information assurance and the security posture of a system or site. AnswerD is incorrect. DITSCAP is a process, which establishes a standard process, a set of activities, general task descriptions, and a management

structure to certify and accredit the IT systems that will maintain the required security posture. Answer: A is incorrect. The NSA- IAM evaluates information systems at a high level and uses a subset of the SSE-CMM process areas to measure the implementation of information security on these systems. Answer: C is incorrect. ASSET is a tool developed by NIST to automate the process of self-assessment through the use of the questionnaire in NIST.

NEW QUESTION: 54
ISO 27003 is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Which of the following elements does this standard contain? Each correct answer represents a complete solution. Choose all that apply.
A. Inter-Organization Co-operation
B. Information Security Risk Treatment
C. CSFs (Critical success factors)
D. ystem requirements for certification bodies Managements
E. Terms and Definitions
F. Guidance on process approach
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: ISO 27003 is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is entitled as "Information Technology - Security techniques - Information security management system implementation guidance".
The ISO 27003 standard provides guidelines for implementing an ISMS (Information Security Management System). It mainly focuses upon the PDCA method along with establishing, implementing, reviewing, and improving the ISMS itself. The ISO 27003 standard contains the following elements: Introduction Scope Terms and Definitions CSFs (Critical success factors) Guidance on process approach Guidance on using PDCA Guidance on Plan Processes Guidance on Do Processes Guidance on Check Processes Guidance on Act Processes Inter-Organization Co-operation AnswerB is incorrect. This element is included in the ISO 27005 standard. AnswerD is incorrect. This element is included in the ISO 27006 standard.

NEW QUESTION: 55
Which of the following processes provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and the security posture of a system or site?
A. NSA-IAM
B. NIACAP
C. ASSET
D. DITSCAP
Answer: B (LEAVE A REPLY)

NIACAP is a process, which provides a standard set of activities, general tasks, and a management structure to certify and accredit systems that maintain the information assurance and the security posture of a system or site. Answer D is incorrect. DITSCAP is a process, which establishes a standard process, a set of activities, general task descriptions, and a management structure to certify and accredit the IT systems that will maintain the required security posture. Answer A is incorrect. The NSA-IAM evaluates information systems at a high level and uses a subset of the SSE-CMM process areas to measure the implementation of information security on these systems. Answer C is incorrect. ASSET is a tool developed by NIST to automate the process of self-assessment through the use of the questionnaire in NIST.

NEW QUESTION: 56
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: 57
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)
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: 58
You are the project manager for GHY Project and are working to create a risk response for a negative risk. You and the project team have identified the risk that the project may not complete on time, as required by the management, due to the creation of the user guide for the software you're creating. You have elected to hire an external writer in order to satisfy the requirements and to alleviate the risk event. What type of risk response have you elected to use in this instance?
A. Transference
B. Exploiting
C. Avoidance
D. Sharing
Answer: A (LEAVE A REPLY)
This is an example of transference as you have transferred the risk to a third party. Transference almost always is done with a negative risk event and it usually requires a contractual
relationship.

NEW QUESTION: 59
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)
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. Answer D 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: 60
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: C (LEAVE A REPLY)

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: 61

A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. What are the different types of policies? Each correct answer represents a complete solution. Choose all that apply.

A. Advisory

B. Systematic

C. Informative
D. Regulatory
Answer: A,C,D (LEAVE A REPLY)
Following are the different types of policies: Regulatory: This type of policy ensures that the organization is following standards set by specific industry regulations. This policy type is very detailed and specific to a type of industry. This is used in financial institutions, health care facilities, public utilities, and other government-regulated industries, e.g., TRAI. Advisory: This type of 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. This policy type can be used, for example, to describe how to handle medical information, handle financial transactions, or process confidential information. Informative: This type of policy informs employees of certain topics. It is not an enforceable policy, but rather one to teach individuals about specific issues relevant to the company. It could explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations. Answer B is incorrect. No such type of policy exists.

NEW QUESTION: 62
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: (SHOW ANSWER)
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: 63
A part of a project deals with the hardware work. As a project manager, you have decided to hire a company to deal with all hardware work on the project. Which type of risk response is this?
A. Exploit
B. Mitigation
C. Transference
D. Avoidance
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: When you are hiring a third party to own risk, it is known as transference risk response.
Transference is a strategy to mitigate negative risks or threats. In this strategy, consequences and the ownership of a risk is transferred to a third party. This strategy does not eliminate the risk but transfers responsibility of managing the risk to another party. Insurance is an example of transference. AnswerB is incorrect. The act of spending money to reduce a risk probability and impact is known as mitigation.
AnswerA is incorrect. Exploit is a strategy that may be selected for risks with positive impacts where the
organization wishes to ensure that the opportunity is realized. AnswerD is incorrect. When extra activities are introduced into the project to avoid the risk, this is an example of avoidance.

NEW QUESTION: 64
Which of the following statements describe the main purposes of a Regulatory policy? Each correct answer represents a complete solution. Choose all that apply.
A. It acknowledges the importance of the computing resources to the business model
B. It provides a statement of support for information security throughout the enterprise
C. It ensures that an organization is following the standard procedures or base practices of operation in its specific industry.
D. It gives an organization the confidence that it is following the standard and accepted industry policy.
Answer: C,D (LEAVE A REPLY)
The main purposes of a Regulatory policy are as follows: It ensures that an organization is following the standard procedures or base practices of operation in its specific industry. It gives an organization the confidence that it is following the standard and accepted industry policy.
Answer B and A are incorrect. These are the policy elements of Senior Management Statement of Policy.

NEW QUESTION: 65
Elizabeth is a project manager for her organization and she finds risk management to be very difficult for her to manage. She asks you, a lead project manager, at what stage in the project will risk management become easier. What answer best resolves the difficulty of risk management practices and the effort required?
A. Risk management only becomes easier when the project moves into project execution.
B. Risk management only becomes easier when the project is closed.
C. Risk management is an iterative process and never becomes easier.
D. Risk management only becomes easier the more often it is practiced.
Answer: D (LEAVE A REPLY)
According to the PMBOK, "Like many things in project management, the more it is done the easier the practice becomes." Answer B is incorrect. This answer is not the best choice for the project. Answer A is incorrect. Risk management likely becomes more difficult in project execution that in other stages of the project. Answer C is incorrect. Risk management does become easier the more often it is done.

NEW QUESTION: 66
Which of the following types of attacks occurs when an attacker successfully inserts an intermediary software or program between two communicating hosts?
A. Denial-of-service attack
B. Dictionary attack
C. Man-in-the-middle attack
D. Password guessing attack
Answer: (SHOW ANSWER)
When an attacker successfully inserts an intermediary software or program between two communicating hosts, it is known as man-in-the-middle attack.

NEW QUESTION: 67
Which of the following access control models uses a predefined set of access privileges for an object of a system?
A. Role-Based Access Control
B. Discretionary Access Control
C. Policy Access Control
D. Mandatory Access Control
Answer: D (LEAVE A REPLY)
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: 68
Which of the following are the benefits of information classification for an organization? Each correct answer represents a complete solution. Choose two.
A. It helps reduce the Total Cost of Ownership (TCO).
B. It helps identify which protections apply to which information.
C. It helps identify which information is the most sensitive or vital to an organization.
D. It ensures that modifications are not made to data by unauthorized personnel or processes.
Answer: B,C (LEAVE A REPLY)
Following are the benefits of information classification for an organization: It helps identify which protections apply to which information. It helps identify which information is the most sensitive or vital to an organization. It supports the tenets of confidentiality, integrity, and availability as it pertains to data. Answer D is incorrect. The concept of integrity ensures that modifications are not made to data by unauthorized personnel or processes. It also ensures that unauthorized modifications are not made to data by authorized personnel or processes. Answer A is incorrect. Information classification cannot reduce the Total Cost of Ownership (TCO).

NEW QUESTION: 69
Which of the following models manages the software development process if the developers are limited to go back only one stage to rework?
A. Waterfall model
B. Spiral model
C. RAD model
D. Prototyping model
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation: In the waterfall model, software development can be managed if the developers are limited to go back only one stage to rework. If this limitation is not imposed mainly on a large project with several team members, then any developer can be working on any phase at any time, and the required rework might be accomplished several times. AnswerB is incorrect. The spiral model is a software development process combining elements of both design and prototyping-in- stages, in an effort to combine advantages of top-down and bottom-up concepts. The basic principles of the spiral model are as follows: The focus is on risk assessment and

minimizing project risks by breaking a project into smaller segments and providing more ease-of-change during the development process, as well as providing the opportunity to evaluate risks and weigh consideration of project continuation throughout the life cycle. Each cycle involves a progression through the same sequence of steps, for each portion of the product and for each of its levels of elaboration, from an overall concept-of-operation document down to the coding of each individual program. Each trip around the spiral traverses the following four basic quadrants: Determine objectives, alternatives, and constraints of the iteration. Evaluate alternatives, and identify and resolve risks. Develop and verify deliverables from the iteration. Plan the next iteration.
Begin each cycle with an identification of stakeholders and their win conditions, and end each cycle with review and commitment. AnswerD is incorrect. The Prototyping model is a systems development method (SDM). In this model, a prototype is created, tested, and then reworked as necessary until an adequate prototype is finally achieved from which the complete system or product can now be developed. Answer C is incorrect. Rapid Application Development (RAD) refers to a type of software development methodology that uses minimal planning in favor of rapid prototyping.

NEW QUESTION: 70
In which of the following testing methodologies do assessors use all available documentation and work under no constraints, and attempt to circumvent the security features of an information system?
A. Full operational test
B. Penetration test
C. Paper test
D. Walk-through test
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. Answer: C is incorrect. A paper test is the least complex test in the disaster recovery and business continuity testing approaches. In this test, the BCP/DRP plan documents are distributed to the appropriate managers and BCP/DRP team members for review, markup, and comment. This approach helps the auditor to ensure that the plan is complete and that all team members are familiar with their responsibilities within the

plan. Answer: D is incorrect. A walk-through test is an extension of the paper testing in the business continuity and disaster recovery process. In this testing methodology, appropriate managers and BCP/DRP team members discuss and walk through procedures of the plan. They also discuss the training needs, and clarification of critical plan elements. Answer: A is incorrect. A full operational test includes all team members and participants in the disaster recovery and business continuity process. This full operation test involves the mobilization of personnel. It restores operations in the same manner as an outage or disaster would. The full operational test extends the preparedness test by including actual notification, mobilization of resources, processing of data, and utilization of backup media for restoration.

NEW QUESTION: 71
The Information System Security Officer (ISSO) and Information System Security Engineer (ISSE) play the role of a supporter and advisor, respectively. Which of the following statements are true about ISSO and ISSE? Each correct answer represents a complete solution. Choose all that apply.
A. An ISSE manages the security of the information system that is slated for Certification & Accreditation (C&A).
B. An ISSE provides advice on the continuous monitoring of the information system.
C. An ISSO manages the security of the information system that is slated for Certification & Accreditation (C&A).
D. An ISSE provides advice on the impacts of system changes.
E. An ISSO takes part in the development activities that are required to implement system changes.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: An Information System Security Officer (ISSO) plays the role of a supporter. The responsibilities of an Information System Security Officer (ISSO) are as follows: Manages the security of the information system that is slated for Certification & Accreditation (C&A). Insures the information systems configuration with the agency's information security policy. Supports the information system owner/information owner for the completion of security-related responsibilities. Takes part in the formal configuration management process. Prepares Certification & Accreditation (C&A) packages. An Information System Security Engineer (ISSE) plays the role of an advisor. The responsibilities of an Information System Security Engineer are as follows: Provides view on the continuous monitoring of the information system. Provides advice on the impacts of system changes. Takes part in the configuration management process. Takes part in the development activities that are required to implement system changes. Follows approved system changes.

NEW QUESTION: 72

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 2, Verification

B. Phase 3, Validation

C. Phase 1, Definition

D. Phase 4, Post Accreditation Phase

Answer: D (LEAVE A REPLY)

Phase 4, Post Accreditation Phase, of the 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. Answer C 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 A 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 B is incorrect. Phase 3 validates the compliance of a fully integrated system with the information stated in the SSAA.

NEW QUESTION: 73

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)

Explanation/Reference:

Explanation: 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: 74

Which of the following describes the acceptable amount of data loss measured in time?

A. Recovery Point Objective (RPO)

B. Recovery Time Objective (RTO)

C. Recovery Consistency Objective (RCO)

D. Recovery Time Actual (RTA)

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation: The Recovery Point Objective (RPO) describes the acceptable amount of data loss measured in time. It is the point in time to which data must be recovered as defined by the organization. The RPO is generally a definition of what an organization determines is an "acceptable loss" in a disaster situation. If the RPO of a company is 2 hours and the time it takes to get the data back into production is 5 hours, the RPO is still 2 hours. Based on this RPO the data must be restored to within 2 hours of the disaster.

AnswerB is incorrect. The Recovery Time Objective (RTO) is the duration of time and a service level

within which a business process must be restored after a disaster or disruption in order to avoid unacceptable consequences associated with a break in business continuity. It includes the time for trying to fix the problem without a recovery, the recovery itself, tests and the communication to the users.

Decision time for user representative is not included. The business continuity timeline usually runs parallel with an incident management timeline and may start at the same, or different, points. In accepted business continuity planning methodology, the RTO is established during the Business Impact Analysis (BIA) by the owner of a process (usually in conjunction with the Business Continuity planner). The RTOs are then presented to senior management for acceptance. The RTO attaches to the business process and not the resources required to support the process. AnswerD is incorrect. The Recovery Time Actual (RTA) is established during an exercise, actual event, or predetermined based on recovery methodology the technology support team develops. This is the time frame the technology support takes to deliver the recovered infrastructure to the business. AnswerC is incorrect. The Recovery Consistency Objective (RCO) is used in Business Continuity Planning in addition to Recovery Point Objective (RPO) and Recovery Time Objective (RTO). It applies data consistency objectives to Continuous Data Protection services.

NEW QUESTION: 75

Which of the following NIST documents provides a guideline for identifying an information system as a National Security System?

A. NIST SP 800-37

B. NIST SP 800-59

C. NIST SP 800-53

D. NIST SP 800-60

E. NIST SP 800-53A

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Explanation: NIST has developed a suite of documents for conducting Certification & Accreditation (C&A).

These documents are as follows: NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems. NIST Special Publication 800-53:
This document provides a guideline for security controls for Federal Information Systems. NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System. NIST Special Publication 800-59: This document is a guideline for identifying an information system as a National Security System. 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: 76
Which of the following models uses a directed graph to specify the rights that a subject can transfer to an object or that a subject can take from another subject?
A. Take-Grant Protection Model
B. Biba Integrity Model
C. Bell-LaPadula Model
D. Access Matrix
Answer: A (LEAVE A REPLY)
The take-grant protection model is a formal model used in the field of computer security to establish or disprove the safety of a given computer system that follows specific rules. It shows that for specific systems the question of safety is decidable in linear time, which is in general undecidable. The model represents a system as directed graph, where vertices are either subjects or objects. The edges between them are labeled and the label indicates the rights that the source of the edge has over the destination. Two rights occur in every instance of the model: take and grant. They play a special role in the graph rewriting rules describing admissible changes of the graph. Answer D is incorrect. The access matrix is a straightforward approach that provides access rights to subjects for objects. Answer C is incorrect. The Bell-LaPadula model deals only with the confidentiality of classified material. It does not address integrity or availability. Answer B is incorrect. The integrity model was developed as an analog to the Bell-LaPadula confidentiality model and then became more sophisticated to address additional integrity requirements.

NEW QUESTION: 77
Which of the following security controls will you use for the deployment phase of the SDLC to build secure software? Each correct answer represents a complete solution. Choose all that apply.
A. Change and Configuration Control
B. Security Certification and Accreditation (C&A)
C. Vulnerability Assessment and Penetration Testing
D. Risk Adjustments
Answer: B,C,D (LEAVE A REPLY)
The various security controls in the SDLC deployment phase are as follows: Secure Installation: While performing any software installation, it should kept in mind that the security configuration of the environment should never be reduced. If it is reduced then security issues and overall risks can affect the environment. Vulnerability Assessment and Penetration Testing: Vulnerability assessments (VA) and penetration testing (PT) is used to determine the risk and attest to the strength of the software after it has been deployed. Security Certification and Accreditation (C&A): Security certification is the process used to ensure controls which are effectively implemented through established verification techniques and procedures, giving organization officials confidence that the appropriate safeguards and countermeasures are in place as means of protection. Accreditation is the provisioning of the necessary security authorization by a senior organization official to process, store, or transmit information. Risk Adjustments: Contingency plans and exceptions should be generated so that the residual risk be above the acceptable threshold.

NEW QUESTION: 78
Which of the following elements sets up a requirement to receive the constrained requests over a protected layer connection, such as TLS (Transport Layer Security)?
A. User data constraint
B. Authorization constraint
C. Web resource collection
D. Accounting constraint
Answer: A (LEAVE A REPLY)
User data constraint is a security constraint element summarized in the Java Servlet Specification 2.4. It sets up a requirement to receive the constrained requests over a protected layer connection, such as TLS (Transport Layer Security). The user data constraint offers guarantee (NONE, INTEGRAL, and CONFEDENTIAL) for the transportation of data between client and server. If a request does not have user data constraint, the container accepts the request after it is received on a connection. Answer C is incorrect. 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 Answer B is incorrect. Authorization constraint is a security constraint element summarized in the Java Servlet Specification 2.4. It sets up a requirement for authentication and names the authorization roles that can access the URL patterns and HTTP methods as defined by the security constraint. In the absence of a security constraint, the container accepts the request without requiring any user authentication. If no authorization role is specified in the authorization constraint, the container cannot access constrained requests. The wildcard character "*" specifies all authorization role names that are defined in the deployment descriptor. Answer D is incorrect. It is not a security constraint element.

NEW QUESTION: 79
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: 80
Which of the following vulnerabilities occurs when an application directly uses or concatenates potentially hostile input with data file or stream functions?
A. Insecure cryptographic storage
B. Malicious file execution
C. Insecure communication
D. Injection flaw

Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: Malicious file execution is a vulnerability that occurs when an application directly uses or concatenates potentially hostile input with data file or stream functions. This leads to arbitrary remote and hostile data being included, processed, and invoked by the Web server. Malicious file execution can be prevented by using an indirect object reference map, input validation, or explicit taint checking mechanism.
AnswerD is incorrect. Injection flaw occurs when data is sent to an interpreter as a part of command or
query. AnswerA is incorrect. Insecure cryptographic storage occurs when applications have failed to encrypt data. Answer: C is incorrect. Insecure communication occurs when applications have failed to encrypt network traffic.

NEW QUESTION: 81
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: (SHOW ANSWER)
ISO/IEC 27002 is an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC) as ISO/IEC 17799:2005. This standard contains the following twelve main sections: 1.Risk assessment: It refers to assessment of risk. 2.Security policy: It deals with the security management. 3.Organization of information security: It deals with governance of information security. 4.Asset management: It refers to inventory and classification of information assets. 5.Human resources security: It deals with security aspects for employees joining, moving and leaving an organization. 6.Physical and environmental security: It is related to protection of the computer facilities. 7.Communications and operations management: It is the management of technical security controls in systems and networks. 8.Access control: It deals with the restriction of access rights to networks, systems, applications, functions and data. 9.Information systems acquisition, development and maintenance: It refers to build security into applications. 10.Information security incident management: It refers to anticipate and respond appropriately to information security breaches. 11.Business continuity management: It deals with protecting, maintaining and recovering business-critical processes and systems. 12.Compliance: It is used for ensuring conformance with information security policies, standards, laws and regulations. Answer C is incorrect. Financial assessment does not come under the ISO/IEC 27002 standard.

NEW QUESTION: 82
Which of the following are the scanning methods used in penetration testing? Each correct answer represents a complete solution. Choose all that apply.

A. Vulnerability
B. Port
C. Services
D. Network
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: The vulnerability, port, and network scanning tools are used in penetration testing. Vulnerability scanning is a process in which a Penetration Tester uses various tools to assess computers, computer systems, networks or applications for weaknesses. There are a number of types of vulnerability scanners available today, distinguished from one another by a focus on particular targets. While functionality varies between different types of vulnerability scanners, they share a common, core purpose of enumerating the vulnerabilities present in one or more targets. Vulnerability scanners are a core technology component of Vulnerability management. Port scanning is the first basic step to get the details of open ports on the target system. Port scanning is used to find a hackable server with a hole or vulnerability. A port is a medium of communication between two computers. Every service on a host is identified by a unique 16-bit number called a port. A port scanner is a piece of software designed to search a network host for open ports. This is often used by administrators to check the security of their networks and by hackers to identify running services on a host with the view to compromising it. Port scanning is used to find the open ports, so that it is possible to search exploits related to that service and application. Network scanning is a penetration testing activity in which a penetration tester or an attacker identifies active hosts on a network, either to attack them or to perform security assessment. A penetration tester uses various tools to identify all the live or responding hosts on the network and their corresponding IP addresses. AnswerC is incorrect. This option comes under vulnerability scanning.

NEW QUESTION: 83
Which of the following is a signature-based intrusion detection system (IDS) ?
A. RealSecure
B. StealthWatch
C. Tripwire
D. Snort
Answer: D (LEAVE A REPLY)
Snort is a signature-based intrusion detection system. Snort is an open source network intrusion prevention and detection system that operates as a network sniffer. It logs activities of the network that is matched with the predefined signatures. Signatures can be designed for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP). The three main modes in which Snort can be configured are as follows: Sniffer mode: It reads the packets of the network and displays them in a continuous stream on the console. Packet logger mode: It logs the packets to the disk. Network intrusion detection mode: It is the most complex and configurable

configuration, allowing Snort to analyze network traffic for matches against a user-defined rule set. Answer B is incorrect. StealthWatch is a behavior-based intrusion detection system. Answer A is incorrect. RealSecure is a network-based IDS that monitors TCP, UDP and ICMP traffic and is configured to look for attack patterns. Answer C is incorrect. Tripwire is a file integrity checker for UNIX/Linux that can be used for host-based intrusion detection.

NEW QUESTION: 84
Who amongst the following makes the final accreditation decision?
A. ISSE
B. CRO
C. DAA
D. ISSO
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: The DAA, also known as Authorizing Official, makes the final accreditation decision. The Designated Approving Authority (DAA), in the United States Department of Defense, is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. The DAA is responsible for implementing system security. The DAA can grant the accreditation and can determine that the system's risks are not at an acceptable level and the system is not ready to be operational. AnswerD 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. AnswerA is incorrect. An Information System Security Engineer (ISSE) plays the role of an advisor. The responsibilities of an Information System Security Engineer are as follows: Provides view on the continuous monitoring of the information system. Provides advice on the impacts of system changes. Takes part in the configuration management process. Takes part in the development activities that are required to implement system changes. Follows approved system changes. AnswerB is incorrect. A Chief Risk Officer (CRO) is also known as Chief Risk Management Officer (CRMO). The Chief Risk Officer or Chief Risk Management Officer of a corporation is the executive accountable for enabling the efficient and effective governance of significant risks, and related opportunities, to a business and its various segments. Risks are commonly categorized as strategic, reputational, operational, financial, or compliance-related. CRO's are accountable to the Executive Committee and The Board for enabling the business to balance risk and reward. In more complex organizations, they are generally responsible for coordinating the organization's Enterprise Risk Management (ERM) approach.

NEW QUESTION: 85

Frank is the project manager of the NHH Project. He is working with the project team to create a plan to document the procedures to manage risks throughout the project. This document will define how risks will be identified and quantified. It will also define how contingency plans will be implemented by the project team. What document is Frank and the NHH Project team creating in this scenario?

A. Risk management plan

B. Project plan

C. Project management plan

D. Resource management plan

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Explanation: The risk management plan, part of the comprehensive management plan, defines how risks will be identified, analyzed, monitored and controlled, and even responded to. A Risk management plan is a document arranged by a project manager to estimate the effectiveness, predict risks, and build response plans to mitigate them. It also consists of the risk assessment matrix. Risks are built in with any project, and project managers evaluate risks repeatedly and build plans to address them. The risk management plan consists of analysis of possible risks with both high and low impacts, and the mitigation strategies to facilitate the project and avoid being derailed through which the common problems arise. Risk management plans should be timely reviewed by the project team in order to avoid having the analysis become stale and not reflective of actual potential project risks. Most critically, risk management plans include a risk strategy for project execution. AnswerC is incorrect. The project management plan is a comprehensive plan that communicates the intent of the project for all project management knowledge areas. Answer B is incorrect. The project plan is not an official PMBOK project management plan. Answer: D is incorrect. The resource management plan defines the management of project resources, such as project team members, facilities, equipment, and contractors.

NEW QUESTION: 86

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

Answer: (SHOW ANSWER)

Explanation/Reference:

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: C 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: 87
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)
Explanation/Reference:
Explanation: 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: 88
FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls have been implemented?
A. Level 2
B. Level 3
C. Level 5
D. Level 1
E. Level 4
Answer: B (LEAVE A REPLY)
The following are the five levels of FITSAF based on SEI's Capability Maturity Model (CMM): Level 1: The first level reflects that an asset has documented a security policy. Level 2: The second level shows that the asset has documented procedures and controls to implement the policy. Level 3: The third level indicates that these procedures and controls have been implemented. Level 4: The fourth level shows that the procedures and controls are tested and reviewed. Level 5: The fifth level is the final level and shows that the asset has procedures and controls fully integrated into a comprehensive program.

NEW QUESTION: 89
Mark works as a Network Administrator for NetTech Inc. He wants users to access only those resources that are required for them. Which of the following access control models will he use?
A. Discretionary Access Control
B. Mandatory Access Control
C. Policy Access Control
D. Role-Based Access Control
E. Explanation:
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: D,E (LEAVE A REPLY)
is incorrect. 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 A is incorrect. DAC is an access control model. In this model, the data owner has the right to decide who can access the data. This model is commonly used in PC environment. The basis of this model is the use of Access Control List (ACL). Answer C is incorrect. There is no such access control model as Policy Access Control.

NEW QUESTION: 90
According to the NIST SAMATE, dynamic analysis tools operate by generating runtime vulnerability scenario using some functions. Which of the following are functions that are used by the dynamic analysis tools and are summarized in the NIST SAMATE? Each correct answer represents a complete solution.
Choose all that apply.
A. Implementation attack
B. Source code security
C. File corruption
D. Network fault injection
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: According to the NIST SAMATE, dynamic analysis tools operate by generating runtime vulnerability scenario using the following functions: Resource fault injection Network fault injection System fault injection User interface fault injection Design attack Implementation attack File corruption AnswerB is incorrect. This function is summarized for static analysis tools.

NEW QUESTION: 91
To help review or design security controls, they can be classified by several criteria . One of these criteria is based on their nature. According to this criterion, which of the following controls consists of incident response processes, management oversight, security awareness, and training?
A. Compliance control
B. Physical control
C. Procedural control
D. Technical control
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: Procedural controls include incident response processes, management oversight, security awareness, and training. Answer: B is incorrect. Physical controls include fences, doors, locks, and fire extinguishers. Answer: D is incorrect. Technical controls include user authentication (login) and logical access controls, antivirus software, and firewalls. Answer: A is incorrect. The legal and regulatory, or compliance controls, include privacy laws, policies, and clauses.

NEW QUESTION: 92
Which of the following plans is a comprehensive statement of consistent actions to be taken before, during, and after a disruptive event that causes a significant loss of information systems resources?
A. Contingency plan
B. Continuity of Operations plan
C. Disaster recovery plan
D. Business Continuity plan
Answer: C (LEAVE A REPLY)
A disaster recovery plan is a complete statement of reliable actions to be taken before, during, and after a disruptive event that causes a considerable loss of information systems resources. The chief objective of a disaster recovery plan is to provide an organized way to make decisions if a disruptive event occurs. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication, and reputation protection, and should refer to the disaster recovery plan (DRP) for IT-related infrastructure recovery/continuity. Answer D is incorrect. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan. Answer B is incorrect. The Continuity Of Operation Plan (COOP) refers to the preparations and institutions maintained by the United States government, providing survival of federal government operations in the case of catastrophic events. It provides procedures and capabilities to sustain an organization's essential. COOP is the procedure documented to ensure persistent critical operations throughout any period where normal operations are unattainable. Answer A is incorrect. A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. 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. They are required to help

governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption.

NEW QUESTION: 93
Which of the following statements best describes the difference between the role of a data owner and the role of a data custodian?
A. The custodian makes the initial information classification assignments, and the operations manager implements the scheme.
B. The data owner implements the information classification scheme after the initial assignment by the custodian.
C. The custodian implements the information classification scheme after the initial assignment by the operations manager.
D. The data custodian implements the information classification scheme after the initial assignment by the data owner.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation: The data owner is responsible for ensuring that the appropriate security controls are in place, for assigning the initial classification to the data to be protected, for approving access requests from other parts of the organization, and for periodically reviewing the data classifications and access rights. Data owners are primarily responsible for determining the data's sensitivity or classification levels, whereas the data custodian has the responsibility for backup, retention, and recovery of data. The data owner delegates these responsibilities to the custodian.
Answer: B, A, and C are incorrect. These are not the valid answers.

NEW QUESTION: 94
The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum standard process for the certification and accreditation of computer and telecommunications systems that handle U.S. national security information. Which of the following participants are required in a NIACAP security assessment? Each correct answer represents a part of the solution. Choose all that apply.
A. Certification agent
B. Designated Approving Authority
C. IS program manager
D. Information Assurance Manager
E. User representative
Answer: A,B,C,E (LEAVE A REPLY)
Explanation/Reference:
Explanation: The NIACAP roles are nearly the same as the DITSCAP roles. Four minimum participants (roles) are required to perform a NIACAP security assessment: IS program manager: The IS program manager is the primary authorization advocate. He is responsible for the Information Systems (IS) throughout the life cycle of the system development. Designated

Approving Authority (DAA): The Designated Approving Authority (DAA), in the United States Department of Defense, is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.
Certification agent: The certification agent is also referred to as the certifier. He provides the technical expertise to conduct the certification throughout the system life cycle. User representative: The user representative focuses on system availability, access, integrity, functionality, performance, and confidentiality in a Certification and Accreditation (C&A) process.
Answer: D is incorrect. Information Assurance Manager (IAM) is one of the key participants in the DIACAP process.

NEW QUESTION: 95
Which of the following fields of management focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life?
A. Configuration management
B. Risk management
C. Change management
D. Procurement management
Answer: A (LEAVE A REPLY)
Configuration management is a field of management that focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life. Configuration Management System is a subsystem of the overall project management system. It is a collection of formal documented procedures used to identify and document the functional and physical characteristics of a product, result, service, or component of the project. It also controls any changes to such characteristics, and records and reports each change and its implementation status. It includes the documentation, tracking systems, and defined approval levels necessary for authorizing and controlling changes. Audits are performed as part of configuration management to determine if the requirements have been met. Answer D is incorrect. The procurement management plan defines more than just the procurement of team members, if needed. It defines how procurements will be planned and executed, and how the organization and the vendor will fulfill the terms of the contract. Answer B 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. Answer C is incorrect. Change Management is used to ensure that standardized methods and procedures are used for efficient handling of all changes.

NEW QUESTION: 96
Martha registers a domain named Microsoft.in. She tries to sell it to Microsoft Corporation. The infringement of which of the following has she made?
A. Copyright

B. Trademark
C. Patent
D. Intellectual property
Answer: (SHOW ANSWER)
According to the Lanham Act, domain names fall under trademarks law. A new section 43(d) of the Trademark Act (Lanham Act) states that anyone who in bad faith registers, traffics in, or uses a domain name that infringes or dilutes another's trademark has committed trademark infringement. Factors involved in assessing bad faith focus on activities typically associated with cyberpiracy or cybersquatting, such as whether the registrant has offered to sell the domain name to the trademark holder for financial gain without having used or intended to use it for a bona fide business; whether the domain-name registrant registered multiple domain names that are confusingly similar to the trademarks of others; and whether the trademark incorporated in the domain name is distinctive and famous. Other factors are whether the domain name consists of the legal name or common handle of the domain-name registrant and whether the domain-name registrant previously used the mark in connection with a bona fide business.

NEW QUESTION: 97
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: (SHOW ANSWER)
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: 98
Which of the following provides an easy way to programmers for writing lower-risk applications and retrofitting security into an existing application?
A. Watermarking
B. Code obfuscation
C. Encryption wrapper
D. ESAPI
Answer: D (LEAVE A REPLY)
ESAPI (Enterprise Security API) is a group of classes that encapsulate the key security operations, needed by most of the applications. It is a free, open source, Web application security control library. ESAPI provides an easy way to programmers for writing lower-risk applications and retrofitting security into an existing application. It offers a solid foundation for new development. Answer C is incorrect. An encryption wrapper is a device that encrypts and decrypts the critical or all software codes at runtime. Answer B is incorrect. Code obfuscation transforms the code so that it is less intelligible for a person. Answer A is incorrect. Watermarking is the irreversible process of embedding information into a digital media. The purpose of digital watermarks is to provide copyright protection for intellectual property that is in digital form.

NEW QUESTION: 99
DRAG DROP
Auditing is used to track user accounts for file and object access, logon attempts, system shutdown, and many more vulnerabilities to enhance the security of the network. It encompasses a wide variety of activities. Place the different auditing activities in front of their descriptions.
Select and Place:
Answer:
Explanation/Reference:
Explanation: Auditing encompasses a wide variety of activities as follows: Logging: It is the activity of recording information to a log file or database about events or occurrences. Log Analysis: It is a systematic form of monitoring where the logged information is analyzed in detail. It is done to find out the trends and patterns as well as abnormal, unauthorized, illegal, and policy-violating activities. Intrusion Detection: It is a process to detect unwanted system access by monitoring both recorded information and real time events.
Alarm Triggers: These are the notifications that are sent to an administrator whenever a specific event occurs. Monitoring: It is the activity of manually or programmatically reviewing logged information.

NEW QUESTION: 100
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: 101
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: (SHOW ANSWER)
Explanation/Reference:
Explanation: NIACAP has four levels of certification. These levels ensure that the appropriate C&A are performed for varying schedule and budget limitations. The certifier must analyze the system's business functions. The certifier determines the degree of confidentiality, integrity, availability, and accountability, and then recommends one of the following NIACAP certification levels: Level 1 - Basic Security Review Level 2 - Minimum Analysis Level 3 - Detailed Analysis Level 4 - Comprehensive Analysis AnswerB and F are incorrect. No such types of levels exist.

NEW QUESTION: 102
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: (SHOW ANSWER)
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: 103
The mission and business process level is the Tier 2. What are the various Tier 2 activities? Each correct answer represents a complete solution. Choose all that apply.
A. Developing an organization-wide information protection strategy and incorporating high-level information security requirements
B. Defining the types of information that the organization needs, to successfully execute the stated missions and business processes
C. Specifying the degree of autonomy for the subordinate organizations
D. Defining the core missions and business processes for the organization
E. Prioritizing missions and business processes with respect to the goals and objectives of the organization
Answer: A,B,C,D,E (LEAVE A REPLY)
The mission and business process level is the Tier 2. It addresses risks from the mission and business process perspective. It is guided by the risk decisions at Tier 1. The various Tier 2 activities are as follows: It defines the core missions and business processes for the organization. It also prioritizes missions and business processes, with respect to the goals and objectives of the

organization. It defines the types of information that an organization requires, to successfully execute the stated missions and business processes. It helps in developing an organization-wide information protection strategy and incorporating high-level information security requirements. It specifies the degree of autonomy for the subordinate organizations.

NEW QUESTION: 104
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: (SHOW ANSWER)
Explanation/Reference:
Explanation: 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. AnswerA 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. AnswerB is incorrect. It deals with the plans and procedures that identify and prioritize the critical business functions that must be preserved. AnswerC 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: 105
Which of the following is designed to detect unwanted attempts at accessing, manipulating, and disabling of computer systems through the Internet?
A. DAS
B. IPsec
C. IDS
D. ACL
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers, malware and/or disgruntled employees. An IDS cannot directly detect attacks within properly encrypted traffic. An intrusion detection system is used to detect several

types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, trojan horses, and worms). Answer: D is incorrect. Access Control List (ACL) is the most commonly used object in Cisco IOS. It filters packets or network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. According to the criteria specified within the access lists, router determines whether the packets to be forwarded or dropped. Access control list criteria could be the source or destination address of the traffic or other information. The types of Cisco ACLs are Standard IP, Extended IP, IPX, Appletalk, etc. Answer: B 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: A is incorrect. Direct-attached storage (DAS) is a digital storage system that is directly attached to a server or workstation, without using a storage network.

NEW QUESTION: 106

Which of the following federal agencies has the objective to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life?

A. National Security Agency (NSA)

B. National Institute of Standards and Technology (NIST)

C. United States Congress

D. Committee on National Security Systems (CNSS)

Answer: B (LEAVE A REPLY)

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 D is incorrect. The Committee on National Security Systems (CNSS) is a United States intergovernmental organization that sets policy for the security of the US security systems. The CNSS holds discussions of policy issues, sets national policy, directions, operational procedures, and guidance for the information systems operated by the U.S. Government, its contractors, or agents that contain classified information, involve intelligence activities, involve cryptographic activities related to national security, etc. Answer A is incorrect. The National Security Agency/Central Security Service (NSA/CSS) is a crypto-logic intelligence agency of the United States government. It is administered as part of the United States Department of Defense. NSA is responsible for the collection and analysis of foreign communications and foreign signals intelligence, which involves cryptanalysis. NSA is also responsible for protecting U.S. government communications and information systems from similar agencies elsewhere, which involves cryptography. NSA is a key component of the U.S. Intelligence Community, which is headed by

the Director of National Intelligence. The Central Security Service is a co-located agency created to coordinate intelligence activities and cooperation between NSA and U.S. military cryptanalysis agencies. NSA's work is limited to communications intelligence. It does not perform field or human intelligence activities. Answer C is incorrect. The United States Congress is the bicameral legislature of the federal government of the United States of America. It consists of the Senate and the House of Representatives. The Congress meets in the United States Capitol in Washington, D.C. Both senators and representatives are chosen through direct election. Each of the 435 members of the House of Representatives represents a district and serves a two-year term. House seats are apportioned among the states by population. The 100 Senators serve staggered six-year terms. Each state has two senators, regardless of population. Every two years, approximately one-third of the Senate is elected at a time. The United States Congress main function is to make laws. The Office of the Law Revision Counsel organizes and publishes the United States Code (USC). It is a consolidation and codification by subject matter of the general and permanent laws of the United States.

NEW QUESTION: 107
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)
Explanation/Reference:
Explanation: 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
AnswerB is incorrect. Information systems acquisition, development, and maintenance is an International
information security standard.

NEW QUESTION: 108
Which of the following describes the acceptable amount of data loss measured in time?
A. Recovery Point Objective (RPO)
B. Recovery Time Objective (RTO)
C. Recovery Consistency Objective (RCO)
D. Recovery Time Actual (RTA)
Answer: A (LEAVE A REPLY)
The Recovery Point Objective (RPO) describes the acceptable amount of data loss measured in time. It is the point in time to which data must be recovered as defined by the organization. The RPO is generally a definition of what an organization determines is an "acceptable loss" in a disaster situation. If the RPO of a company is 2 hours and the time it takes to get the data back into production is 5 hours, the RPO is still 2 hours. Based on this RPO the data must be restored to within 2 hours of the disaster. Answer B is incorrect. The Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster or disruption in order to avoid unacceptable consequences associated with a break in business continuity. It includes the time for trying to fix the problem without a recovery, the recovery itself, tests and the communication to the users. Decision time for user representative is not included. The business continuity timeline usually runs parallel with an incident management timeline and may start at the same, or different, points. In accepted business continuity planning methodology, the RTO is established during the Business Impact Analysis (BIA) by the owner of a process (usually in conjunction with the Business Continuity planner). The RTOs are then presented to senior management for acceptance. The RTO attaches to the business process and not the resources required to support the process. Answer D is incorrect. The Recovery Time Actual (RTA) is established during an exercise, actual event, or predetermined based on recovery methodology the technology support team develops. This is the time frame the technology support takes to deliver the recovered infrastructure to the business. Answer C is incorrect. The Recovery Consistency Objective (RCO) is used in Business Continuity Planning in addition to Recovery Point Objective (RPO) and Recovery Time Objective (RTO). It applies data consistency objectives to Continuous Data Protection services.

NEW QUESTION: 109
Which of the following tools is used to attack the Digital Watermarking?
A. Steg-Only Attack
B. Active Attacks
C. 2Mosaic

D. Gifshuffle

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation: 2Mosaic is a tool used for watermark breaking. It is an attack against a digital watermarking system. In this type of attack, an image is chopped into small pieces and then placed together. When this image is embedded into a web page, the web browser renders the small pieces into one image. This image looks like a real image with no watermark in it. This attack is successful, as it is impossible to read watermark in very small pieces. Answer: D is incorrect. Gifshuffle is used to hide message or information inside GIF images. It is done by shuffling the colormap. This tool also provides compression and encryption. Answer: B and A are incorrect. Active Attacks and Steg-Only Attacks are used to attack Steganography.

NEW QUESTION: 110

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

A. File-based

B. Network-based

C. Anomaly-based

D. Signature-based

E. Explanation:

The anomaly-based intrusion detection system (IDS) monitors network traffic and compares it against an established baseline. This type of IDS monitors traffic and system activity for unusual behavior based on statistics. In order to identify a malicious activity, it learns normal behavior from the baseline. The anomaly-based intrusion detection is also known as behavior-based or statistical-based intrusion detection.

Answer: C (LEAVE A REPLY)

is incorrect. Signature-based IDS uses a database with signatures to identify possible attacks and malicious activity. Answer B is incorrect. A network-based IDS can be a dedicated hardware appliance, or an application running on a computer, attached to the network. It monitors all traffic in a network or traffic coming through an entry-point such as an Internet connection. Answer A is incorrect. There is no such intrusion detection system (IDS) that is file-based.

NEW QUESTION: 111

Which of the following elements of BCP process includes the areas of plan implementation, plan testing, and ongoing plan maintenance, and also involves defining and documenting the continuity strategy?

A. Business continuity plan development

B. Business impact assessment

C. Scope and plan initiation

D. Plan approval and implementation

Answer: A (LEAVE A REPLY)

Explanation/Reference:
Explanation: 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: C is incorrect. 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: B 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: D 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: 112
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)
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. Answer B 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: 113

Which of the following is an attack with IP fragments that cannot be reassembled?

A. Password guessing attack

B. Teardrop attack

C. Dictionary attack

D. Smurf attack

Answer: B (LEAVE A REPLY)

Teardrop is an attack with IP fragments that cannot be reassembled. In this attack, corrupt packets are sent to the victim's computer by using IP's packet fragmentation algorithm. As a result of this attack, the victim's computer might hang. Answer D is incorrect. Smurf is an ICMP attack that involves spoofing and flooding. Answer C is incorrect. Dictionary attack is a type of password guessing attack. This type of attack uses a dictionary of common words to find out the password of a user. It can also use common words in either upper or lower case to find a password. There are many programs available on the Internet to automate and execute dictionary attacks. Answer A is incorrect. A password guessing attack occurs when an unauthorized user tries to log on repeatedly to a computer or network by guessing usernames and passwords. Many password guessing programs that attempt to break passwords are available on the Internet. Following are the types of password guessing attacks: Brute force attack Dictionary attack

NEW QUESTION: 114

FIPS 199 defines the three levels of potential impact on organizations. Which of the following potential impact levels shows limited adverse effects on organizational operations, organizational assets, or individuals?

A. Moderate

B. Low

C. Medium

D. High

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation: The potential impact is called low if the loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Answer: C is incorrect. Such a type of potential impact level does not exist Answer: A is incorrect. The potential impact is known to be moderate if the loss of confidentiality, integrity, or availability is expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Answer: D is incorrect. The potential impact is called high if the loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

NEW QUESTION: 115

Which of the following fields of management focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life?

A. Configuration management
B. Risk management
C. Change management
D. Procurement management
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation: Configuration management is a field of management that focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life. Configuration Management System is a subsystem of the overall project management system. It is a collection of formal documented procedures used to identify and document the functional and physical characteristics of a product, result, service, or component of the project. It also controls any changes to such characteristics, and records and reports each change and its implementation status. It includes the documentation, tracking systems, and defined approval levels necessary for authorizing and controlling changes. Audits are performed as part of configuration management to determine if the requirements have been met. AnswerD is incorrect. The procurement management plan defines more than just the procurement of team members, if needed. It defines how procurements will be planned and executed, and how the organization and the vendor will fulfill the terms of the contract. Answer B 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. Answer: C is incorrect. Change Management is used to ensure that standardized methods and procedures are used for efficient handling of all changes.

NEW QUESTION: 116
You work as a Security Manager for Tech Perfect Inc. In the organization, Syslog is used for computer system management and security auditing, as well as for generalized informational, analysis, and debugging messages. You want to prevent a denial of service (DoS) for the Syslog server and the loss of Syslog messages from other sources. What will you do to accomplish the task?
A. Use a different message format other than Syslog in order to accept data.
B. Enable the storage of log entries in both traditional Syslog files and a database.
C. Limit the number of Syslog messages or TCP connections from a specific source for a certain time period.
D. Encrypt rotated log files automatically using third-party or OS mechanisms.
Answer: C (LEAVE A REPLY)
In order to accomplish the task, you should limit the number of Syslog messages or TCP connections from a specific source for a certain time period. This will prevent a denial of service (DoS) for the Syslog server and the loss of Syslog messages from other sources. Answer D is incorrect. You can encrypt rotated log files automatically using third-party or OS mechanisms to protect data confidentiality. Answer A is incorrect. You can use a different message format other

than Syslog in order to accept data for aggregating data from hosts that do not support Syslog. Answer B is incorrect. You can enable the storage of log entries in both traditional Syslog files and a database for creating a database storage for logs.

NEW QUESTION: 117
The NIST Information Security and Privacy Advisory Board (ISPAB) paper "Perspectives on Cloud Computing and Standards" specifies potential advantages and disdvantages of virtualization. Which of the following disadvantages does it include? Each correct answer represents a complete solution. Choose all that apply.
A. It increases capabilities for fault tolerant computing using rollback and snapshot features.
B. It increases intrusion detection through introspection.
C. It initiates the risk that malicious software is targeting the VM environment.
D. It increases overall security risk shared resources.
E. It creates the possibility that remote attestation may not work.
F. It involves new protection mechanisms for preventing VM escape, VM detection, and VM-VM interference.
G. It increases configuration effort because of complexity and composite system.
Answer: C,D,E,F,G (LEAVE A REPLY)
The potential security disadvantages of virtualization are as follows: It increases configuration effort because of complexity and composite system. It initiates the problem of how to prevent overlap while mapping VM storage onto host files. It introduces the problem of virtualizing the TPM. It creates the possibility that remote attestation may not work. It initiates the problem of detecting VM covert channels. It involves new protection mechanisms for preventing VM escape, VM detection, and VM-VM interference. It initiates the possibility of virtual networking configuration errors. It initiates the risk that malicious software is targeting the VM environment. It increases overall security risk shared resources, such as networks, clipboards, clocks, printers, desktop management, and folders. Answer A and B are incorrect. These are not the disadvantages of virtualization, as described in the NIST Information Security and Privacy Advisory Board (ISPAB) paper "Perspectives on Cloud Computing and Standards".

NEW QUESTION: 118
You work as a Network Administrator for uCertify Inc. You need to secure web services of your company in order to have secure transactions. Which of the following will you recommend for providing security?
A. SSL
B. VPN
C. S/MIME
D. HTTP
Answer: (SHOW ANSWER)
The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer

Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. URLs that require an SSL connection start with https: instead of http:. Answer C is incorrect. S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of e- mail encapsulated in MIME. S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity, non-repudiation of origin (using digital signatures), privacy, and data security (using encryption). Answer D is incorrect. Hypertext Transfer Protocol (HTTP) is a client/server TCP/IP protocol used on the World Wide Web (WWW) to display Hypertext Markup Language (HTML) pages. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when a client application or browser sends a request to the server using HTTP commands, the server responds with a message containing the protocol version, success or failure code, server information, and body content, depending on the request. HTTP uses TCP port 80 as the default port. Answer B is incorrect. A Virtual Private Network (VPN) is a computer network that is implemented in an additional software layer (overlay) on top of an existing larger network for the purpose of creating a private scope of computer communications or providing a secure extension of a private network into an insecure network such as the Internet. The links between nodes of a Virtual Private Network are formed over logical connections or virtual circuits between hosts of the larger network. The Link Layer protocols of the virtual network are said to be tunneled through the underlying transport network.

NEW QUESTION: 119

You work as a CSO (Chief Security Officer) for Tech Perfect Inc. You have a disaster scenario and you want to discuss it with your team members for getting appropriate responses of the disaster. In which of the following disaster recovery tests can this task be performed?

A. Structured walk-through test

B. Full-interruption test

C. Parallel test

D. Simulation test

Answer: D (LEAVE A REPLY)

A simulation test is a method used to test the disaster recovery plans. It operates just like a structured walk-through test. In the simulation test, the members of a disaster recovery team present with a disaster scenario and then, discuss on appropriate responses. These suggested responses are measured and some of them are taken by the team. The range of the simulation test should be defined carefully for avoiding excessive disruption of normal business activities. Answer A is incorrect. The structured walk-through test is also known as the table-top exercise. In structured walk-through test, the team members walkthrough the plan to identify and correct weaknesses and how they will respond to the emergency scenarios by stepping in the course of the plan. It is the most effective and competent way to identify the areas of overlap in the plan before conducting more challenging training exercises. Answer B is incorrect. A full-interruption

test includes the operations that shut down at the primary site and are shifted to the recovery site according to the disaster recovery plan. It operates just like a parallel test. The full-interruption test is very expensive and difficult to arrange. Sometimes, it causes a major disruption of operations if the test fails. Answer C is incorrect. A parallel test includes the next level in the testing procedure, and relocates the employees to an alternate recovery site and implements site activation procedures. These employees present with their disaster recovery responsibilities as they would for an actual disaster. The disaster recovery sites have full responsibilities to conduct the day-to-day organization's business.

NEW QUESTION: 120
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: 121
In which of the following deployment models of cloud is the cloud infrastructure operated exclusively for an organization?
A. Public cloud
B. Community cloud
C. Private cloud
D. Hybrid cloud
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: In private cloud, the cloud infrastructure is operated exclusively for an organization. The private cloud infrastructure is administered by the organization or a third party, and exists on premise and off premise.

NEW QUESTION: 122
Which of the following statements about the integrity concept of information security management are true? Each correct answer represents a complete solution. Choose three.
A. It ensures that unauthorized modifications are not made to data by authorized personnel or processes.
B. It determines the actions and behaviors of a single individual within a system
C. It ensures that internal information is consistent among all subentities and also consistent with the real-world, external situation.
D. It ensures that modifications are not made to data by unauthorized personnel or processes.
Answer: A,C,D (LEAVE A REPLY)
The following statements about the integrity concept of information security management are true: It ensures that modifications are not made to data by unauthorized personnel or processes. It ensures that unauthorized modifications are not made to data by authorized personnel or processes. It ensures that internal information is consistent among all subentities and also consistent with the real-world, external situation. Answer B is incorrect. Accountability determines the actions and behaviors of an individual within a system, and identifies that particular individual. Audit trails and logs support accountability.

NEW QUESTION: 123
Which of the following specifies the behaviors of the DRM implementation and any applications that are accessing the implementation?
A. OS fingerprinting
B. OTA provisioning
C. Access control
D. Compliance rule
Answer: (SHOW ANSWER)
The Compliance rule specifies the behaviors of the DRM implementation and any applications that are accessing the implementation. The compliance rule specifies the following elements: Definition of specific license rights Device requirements Revocation of license path or penalties when the implementation is not robust enough or noncompliant Answer B is incorrect. 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. Answer C is incorrect. An access control is a system, which enables an authority to control access to areas and resources in a given physical facility, or computer-based information system. Access control system, within the field of physical security, is generally seen as the second layer in the security of a physical

structure. It refers to all mechanisms that control visibility of screens, views, and data within Siebel Business Applications. Answer A is incorrect. OS fingerprinting is a process in which an external host sends special traffic on the external network interface of a computer to determine the computer's operating system. It is one of the primary steps taken by hackers in preparing an attack.

NEW QUESTION: 124
Which of the following coding practices are helpful in simplifying code? Each correct answer represents a complete solution. Choose all that apply.
A. Programmers should use multiple small and simple functions rather than a single complex function.
B. Software should avoid ambiguities and hidden assumptions, recursions, and GoTo statements.
C. Programmers should implement high-consequence functions in minimum required lines of code and follow proper coding standards.
D. Processes should have multiple entry and exit points.
Answer: A,B,C (LEAVE A REPLY)
Explanation/Reference:
Explanation: The various coding practices that are helpful in simplifying the code are as follows: Programmers should implement high-consequence functions in minimum required lines of code and follow the proper coding standards. Software should implement the functions that are defined in the software specification. Software should avoid ambiguities and hidden assumptions, recursion, and GoTo statements. Programmers should use multiple small and simple functions rather than a complex function.
The processes should have only one entry point and minimum exit points. Interdependencies should be minimum so that a process module or component can be disabled when it is not needed, or replaced when it is found insecure or a better alternative is available, without disturbing the software operations.
Programmers should use object-oriented techniques to keep the code simple and small. Some of the object-oriented techniques are object inheritance, encapsulation, and polymorphism. Answer: D is incorrect. Processes should have only one entry point and the minimum number of exit points.

NEW QUESTION: 125
Which of the following are the levels of public or commercial data classification system? Each correct answer represents a complete solution. Choose all that apply.
A. Sensitive
B. Private
C. Unclassified
D. Confidential
E. Secret
F. Public

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation: The public or commercial data classification is also built upon a four-level model, which are as follows: Public Sensitive Private Confidential Each level (top to bottom) represents an increasing level of sensitivity. The public level is similar to unclassified level military classification system. This level of data should not cause any damage if disclosed. Sensitive is a higher level of classification than public level data. This level of data requires a greater level of protection to maintain confidentiality. The Private level of data is intended for company use only. Disclosure of this level of data can damage the company. The Confidential level of data is considered very sensitive and is intended for internal use only. Disclosure of this level of data can cause serious damage to the company. AnswerC and E are incorrect. Unclassified and secret are the levels of military data classification.

NEW QUESTION: 126

Certification and Accreditation (C&A or CnA) is a process for implementing information security. Which of the following is the correct order of C&A phases in a DITSCAP assessment?

A. Verification, Definition, Validation, and Post Accreditation

B. Definition, Validation, Verification, and Post Accreditation

C. Definition, Verification, Validation, and Post Accreditation

D. Verification, Validation, Definition, and Post Accreditation

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation: C&A consists of four phases in a DITSCAP assessment. These phases are the same as NIACAP phases. The order of these phases is as follows: 1.Definition: The definition phase is focused on understanding the IS business case, the mission, environment, and architecture. This phase determines the security requirements and level of effort necessary to achieve Certification & Accreditation (C&A).

2.Verification: The second phase confirms the evolving or modified system's compliance with the information. The verification phase ensures that the fully integrated system will be ready for certification testing. 3.Validation: The third phase confirms abidance of the fully integrated system with the security policy. This phase follows the requirements slated in the SSAA. The objective of the validation phase is to show the required evidence to support the DAA in accreditation process. 4.Post Accreditation: The Post Accreditation is the final phase of DITSCAP assessment and it starts after the system has been certified and accredited for operations. This phase ensures secure system management, operation, and maintenance to save an acceptable level of residual risk.

NEW QUESTION: 127

The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise. What are the responsibilities of a

Chief Information Officer? Each correct answer represents a complete solution. Choose all that apply.

A. Facilitating the sharing of security risk-related information among authorizing officials

B. Preserving high-level communications and working group relationships in an organization

C. Establishing effective continuous monitoring program for the organization

D. Proposing the information technology needed by an enterprise to achieve its goals and then working within a budget to implement the plan

E. Explanation:

A Chief Information Officer (CIO) plays the role of a leader. The responsibilities of a Chief Information Officer are as follows: Establishes effective continuous monitoring program for the organization. Facilitates continuous monitoring process for the organizations. Preserves high-level communications and working group relationships in an organization. Confirms that information systems are covered by a permitted security plan and monitored throughout the System Development Life Cycle (SDLC). Manages and delegates decisions to employees in large enterprises. Proposes the information technology needed by an enterprise to achieve its goals and then works within a budget to implement the plan.

Answer: B,C,D,E (LEAVE A REPLY)

is incorrect. A Risk Executive facilitates the sharing of security risk-related information among authorizing officials.

NEW QUESTION: 128

Which of the following security controls works as the totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy?

A. Common data security architecture (CDSA)

B. Application program interface (API)

C. Trusted computing base (TCB)

D. Internet Protocol Security (IPSec)

Answer: C (LEAVE A REPLY)

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. Answer D is incorrect. Internet Protocol Security (IPSec) is a standard-based protocol that provides the highest level of VPN security. IPSec can encrypt virtually everything above the networking layer. It is used for VPN connections that use the L2TP protocol. It secures both data and password. IPSec cannot be used with Point-to-Point Tunneling Protocol (PPTP). Answer A is incorrect. The Common data security architecture (CDSA) is a set of layered security services and cryptographic framework. It deals with the communications and data security problems in the emerging Internet and intranet application space. It presents an infrastructure for building cross-platform, interoperable, security-enabled applications for client-server environments. Answer B is incorrect. An application programming interface (API) is an interface implemented by a software

program which enables it to interact with other software. It facilitates interaction between different software programs similar to the way the user interface facilitates interaction between humans and computers. An API is implemented by applications, libraries, and operating systems to determine their vocabularies and calling conventions, and is used to access their services. It may include specifications for routines, data structures, object classes, and protocols used to communicate between the consumer and the implementer of the API.

NEW QUESTION: 129
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: 130
Henry is the project manager of the QBG Project for his company. This project has a budget of $4,576,900 and is expected to last 18 months to complete. The CIO, a stakeholder in the project, has introduced a scope change request for additional deliverables as part of the project work. What component of the change control system would review the proposed changes' impact on the features and functions of the project's product?
A. Configuration management system
B. Scope change control system
C. Cost change control system
D. Integrated change control
Answer: (SHOW ANSWER)
The configuration management system ensures that proposed changes to the project's scope are reviewed and evaluated for their affect on the project's product. Configuration Management System is a subsystem of the overall project management system. It is a collection of formal

documented procedures used to identify and document the functional and physical characteristics of a product, result, service, or component of the project. It also controls any changes to such characteristics, and records and reports each change and its implementation status. It includes the documentation, tracking systems, and defined approval levels necessary for authorizing and controlling changes. Audits are performed as part of configuration management to determine if the requirements have been met. Answer B is incorrect. The scope change control system focuses on reviewing the actual changes to the project scope. When a change to the project's scope is proposed, the configuration management system is also invoked. Answer C is incorrect. The cost change control system is responsible for reviewing and controlling changes to the project costs. Answer D is incorrect. Integrated change control examines the affect of a proposed change on the project as a whole.

NEW QUESTION: 131
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He finds that the We-are-secure server is vulnerable to attacks. As a countermeasure, he suggests that the Network Administrator should remove the IPP printing capability from the server. He is suggesting this as a countermeasure against _____.
A. SNMP enumeration
B. IIS buffer overflow
C. NetBIOS NULL session
D. DNS zone transfer
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: Removing the IPP printing capability from a server is a good countermeasure against an IIS buffer overflow attack. A Network Administrator should take the following steps to prevent a Web server from IIS buffer overflow attacks: Conduct frequent scans for server vulnerabilities. Install the upgrades of Microsoft service packs.
Implement effective firewalls. Apply URLScan and IISLockdown utilities. Remove the IPP printing capability. AnswerD is incorrect. The following are the DNS zone transfer countermeasures: Do not allow DNS zone transfer using the DNS property sheet: a.Open DNS. b.Right-click a DNS zone and click Properties. c.On the Zone Transfer tab, clear the Allow zone transfers check box. Configure the master DNS server to allow zone transfers only from secondary DNS servers: a.Open DNS. b.Right-click a DNS zone and click Properties. c.On the zone transfer tab, select the Allow zone transfers check box, and then do one of the following: To allow zone transfers only to the DNS servers listed on the name servers tab, click on the Only to the servers listed on the Name Server tab. To allow zone transfers only to specific DNS servers, click Only to the following servers, and add the IP address of one or more servers. Deny all unauthorized inbound connections to TCP port 53. Implement DNS keys and encrypted DNS payloads.
AnswerA is incorrect. The following are the countermeasures against SNMP enumeration:
1.Removing

the SNMP agent or disabling the SNMP service 2.Changing the default PUBLIC community name when
'shutting off SNMP' is not an option 3.Implementing the Group Policy security option called Additional restrictions for anonymous connections 4.Restricting access to NULL session pipes and NULL session shares 5.Upgrading SNMP Version 1 with the latest version 6.Implementing Access control list filtering to allow only access to the read-write community from approved stations or subnets AnswerC is incorrect.
NetBIOS NULL session vulnerabilities are hard to prevent, especially if NetBIOS is needed as part of the infrastructure. One or more of the following steps can be taken to limit NetBIOS NULL session vulnerabilities: 1.Null sessions require access to the TCP 139 or TCP 445 port, which can be disabled by a Network Administrator. 2.A Network Administrator can also disable SMB services entirely on individual hosts by unbinding WINS Client TCP/IP from the interface. 3.A Network Administrator can also restrict the anonymous user by editing the registry values: a.Open regedit32, and go to HKLM\SYSTEM
\CurrentControlSet\LSA. b.Choose edit > add value. Value name: RestrictAnonymous Data Type: REG_WORD Value: 2

NEW QUESTION: 132
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)
Explanation/Reference:
Explanation: 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: 133
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: (SHOW ANSWER)
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: 134
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: D (LEAVE A REPLY)
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: 135
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: 136
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)
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: 137
You are the project manager of the CUL project in your organization. You and the project team are assessing the risk events and creating a probability and impact matrix for the identified risks. Which one of the following statements best describes the requirements for the data type used in qualitative risk analysis?
A. A qualitative risk analysis encourages biased data to reveal risk tolerances.
B. A qualitative risk analysis required unbiased stakeholders with biased risk tolerances.
C. A qualitative risk analysis requires accurate and unbiased data if it is to be credible.
D. A qualitative risk analysis requires fast and simple data to complete the analysis.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: Of all the choices only this answer is accurate. The PMBOK clearly states that the data must be accurate and unbiased to be credible. Answer: D is incorrect. This is not a valid statement about the qualitative risk analysis data. Answer: A is incorrect. This is not a valid statement about the qualitative risk analysis data. Answer: B is incorrect. This is not a valid statement about the qualitative risk analysis data.

NEW QUESTION: 138
CORRECT TEXT
Fill in the blank with an appropriate phrase. models address specifications, requirements, design, verification and validation, and maintenance activities.
A. Life cycle
Answer: A (LEAVE A REPLY)
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: 139
According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Which of the following are

among the eight areas of IA defined by DoD? Each correct answer represents a complete solution. Choose all that apply.

A. VI Vulnerability and Incident Management

B. Information systems acquisition, development, and maintenance

C. DC Security Design & Configuration

D. EC Enclave and Computing Environment

Answer: A,C,D (LEAVE A REPLY)

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

NEW QUESTION: 140

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: C (LEAVE A REPLY)

Explanation/Reference:

Explanation: Non repudiation refers to mechanisms that prevent a party from falsely denying involvement in some data transaction.

NEW QUESTION: 141

Which of the following testing methods verifies the interfaces between components against a software design?

A. Regression testing

B. Integration testing

C. Black-box testing

D. Unit testing

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Explanation: Integration testing is a software testing that seeks to verify the interfaces between components against a software design. Software components may be integrated in an iterative way or all together ("big bang"). Normally the former is considered a better practice since it allows interface issues to be localized more quickly and fixed. Integration testing works to expose

defects in the interfaces and interaction between the integrated components (modules). Progressively larger groups of tested software components corresponding to elements of the architectural design are integrated and tested until the software works as a system. Answer: A is incorrect. Regression testing focuses on finding defects after a major code change has occurred. Specifically, it seeks to uncover software regressions, or old bugs that have come back. Such regressions occur whenever software functionality that was previously working correctly stops working as intended. Typically, regressions occur as an unintended consequence of program changes, when the newly developed part of the software collides with the previously existing code. Answer: D is incorrect. Unit testing refers to tests that verify the functionality of a specific section of code, usually at the function level. In an object-oriented environment, this is usually at the class level, and the minimal unit tests include the constructors and destructors. These types of tests are usually written by developers as they work on code (white-box style), to ensure that the specific function is working as expected. One function might have multiple tests, to catch corner cases or other branches in the code. Unit testing alone cannot verify the functionality of a piece of software, but rather is used to assure that the building blocks the software uses work independently of each other. Answer: C is incorrect. The black-box testing uses external descriptions of the software, including specifications, requirements, and design to derive test cases. These tests can be functional or non-functional, though usually functional. The test designer selects valid and invalid inputs and determines the correct output. There is no knowledge of the test object's internal structure. This method of test design is applicable to all levels of software testing: unit, integration, functional testing, system and acceptance. The higher the level, and hence the bigger and more complex the box, the more one is forced to use black box testing to simplify. While this method can uncover unimplemented parts of the specification, one cannot be sure that all existent paths are tested.

NEW QUESTION: 142
Which of the following provides an easy way to programmers for writing lower-risk applications and retrofitting security into an existing application?
A. Watermarking
B. ESAPI
C. Encryption wrapper
D. Code obfuscation
Answer: (SHOW ANSWER)
ESAPI (Enterprise Security API) is a group of classes that encapsulate the key security operations, needed by most of the applications. It is a free, open source, Web application security control library. ESAPI provides an easy way to programmers for writing lower-risk applications and retrofitting security into an existing application. It offers a solid foundation for new development. Answer A is incorrect. Watermarking is the process of embedding information into software in a way that is difficult to remove. Answer C is incorrect. Encryption wrapper dynamically encrypts and decrypts all the software code at runtime. Answer D is incorrect. Code obfuscation is designed to protect code from decompilation.

NEW QUESTION: 143
Which of the following is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention?
A. Copyright
B. Snooping
C. Utility model
D. Patent
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: A patent is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention. Answer: A 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 B is incorrect. Snooping is an activity of observing the content that appears on a computer monitor
or watching what a user is typing. Snooping also occurs by using software programs to remotely monitor activity on a computer or network device. Hackers or attackers use snooping techniques and equipment such as keyloggers to monitor keystrokes, capture passwords and login information, and to intercept e- mail and other private communications. Sometimes, organizations also snoop their employees legitimately to monitor their use of organizations' computers and track Internet usage. Answer: C is incorrect. A utility model is an intellectual property right to protect inventions.

NEW QUESTION: 144
Which of the following is a variant with regard to Configuration Management?
A. A CI that has the same name as another CI but shares no relationship.
B. A CI that particularly refers to a software version.
C. A CI that has the same essential functionality as another CI but a bit different in some small manner.
D. A CI that particularly refers to a hardware specification.
Answer: C (LEAVE A REPLY)
A CI that has the same essential functionality as another CI but a bit different in some small manner, and therefore, might be required to be analyzed along with its generic group. A Configuration item (CI) is an IT asset or a combination of IT assets that may depend and have relationships with other IT processes. A CI will have attributes which may be hierarchical and relationships that will be assigned by the configuration manager in the CM database. The Configuration Item (CI) attributes are as follows: 1.Technical: It is data that describes the CI's

capabilities which include software version and model numbers, hardware and manufacturer specifications, and other technical details like networking speeds, and data storage size. Keyboards, mice and cables are considered consumables. 2.Ownership: It is part of financial asset management, ownership attributes, warranty, location, and responsible person for the CI. 3.Relationship: It is the relationship among hardware items, software, and users. Answer B, D, and A are incorrect. These are incorrect definitions of a variant with regard to Configuration Management.

NEW QUESTION: 145
Billy is the project manager of the HAR Project and is in month six of the project. The project is scheduled to last for 18 months. Management asks Billy how often the project team is participating in risk reassessment in this project. What should Billy tell management if he's following the best practices for risk management?
A. Project risk management happens at every milestone.
B. Project risk management has been concluded with the project planning.
C. Project risk management is scheduled for every month in the 18-month project.
D. At every status meeting the project team project risk management is an agenda item.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Risk management is an ongoing project activity. It should be an agenda item at every project status meeting. AnswerA 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: 146
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: A,B,C,D,E (LEAVE A REPLY)
Explanation/Reference:
Explanation: 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 AnswerF is incorrect. It is a part of Administrative Controls.

NEW QUESTION: 147
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: 148
Which of the following statements best describes the difference between the role of a data owner and the role of a data custodian?
A. The custodian makes the initial information classification assignments, and the operations manager implements the scheme.
B. The data owner implements the information classification scheme after the initial assignment by the custodian.
C. The custodian implements the information classification scheme after the initial assignment by the operations manager.
D. The data custodian implements the information classification scheme after the initial assignment by the data owner.
Answer: D (LEAVE A REPLY)
The data owner is responsible for ensuring that the appropriate security controls are in place, for assigning the initial classification to the data to be protected, for approving access requests from other parts of the organization, and for periodically reviewing the data classifications and access rights. Data owners are primarily responsible for determining the data's sensitivity or classification levels, whereas the data custodian has the responsibility for backup, retention, and recovery of data. The data owner delegates these responsibilities to the custodian. Answer B, A, and C are incorrect. These are not the valid answers.

NEW QUESTION: 149
Which of the following testing methods tests the system efficiency by systematically selecting the suitable and minimum set of tests that are required to effectively cover the affected changes?
A. Unit testing
B. Integration testing
C. Acceptance testing
D. Regression testing
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation: Regression testing focuses on finding defects after a major code change has occurred.
Specifically, it seeks to uncover software regressions, or old bugs that have come back. Such regressions occur whenever software functionality that was previously working correctly stops working as intended.
Typically, regressions occur as an unintended consequence of program changes, when the newly developed part of the software collides with the previously existing code. Regression testing tests the system efficiency by systematically selecting the suitable and minimum set of tests that are required to effectively cover the affected changes. Answer: A 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. Answer: C is incorrect.
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: B is incorrect. Integration testing is a software testing that seeks to verify the interfaces between components against a software design. Software components may be integrated in an iterative way or all together ("big bang"). Normally the former is considered a better practice since it allows interface issues to be localized more quickly and fixed. Integration testing works to expose defects in the interfaces and interaction between the integrated components (modules).
Progressively larger groups of tested software components corresponding to elements of the architectural design are integrated and tested until the software works as a system.

NEW QUESTION: 150
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: 151
In which of the following SDLC phases is the system's security features configured and enabled, the system is tested and installed or fielded, and the system is authorized for processing?
A. Development/Acquisition Phase
B. Operation/Maintenance Phase
C. Implementation Phase
D. Initiation Phase
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: It is the implementation phase, in which the system's security features are configured and enabled, the system is tested and installed or fielded, and the system is authorized for processing. A design review and systems test should be performed prior to placing the system into operation to ensure that it meets security specifications. AnswerB is incorrect. In Operation/Maintenance Phase, the system performs its work. The system is almost always being continuously modified by the addition of hardware and software and by numerous other events. Answer D is incorrect. In the initiation phase, the need for a system is expressed and the purpose of the system is documented. Answer: A is incorrect. In Development/Acquisition Phase, the system is designed, purchased, programmed, developed, or otherwise constructed.

NEW QUESTION: 152
An assistant from the HR Department calls you to ask the Service Hours & Maintenance Slots for your ERP system. In which document will you most probably find this information?

A. Service Level Agreement
B. Release Policy
C. Service Level Requirements
D. Underpinning Contract
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation: You will most probably find this information in the Service Level Agreement document.
Amongst other information, SLA contains information about the agreed Service Hours and maintenance slots for any particular Service. Service Level Agreement (frequently abbreviated as SLA) is a part of a service contract where the level of service is formally defined. In practice, the term SLA is sometimes used to refer to the contracted delivery time (of the service) or performance. Service Level Agreement (SLA) is a negotiated agreement between two parties where one is the customer and the other is the service provider. This can be a legally binding formal or informal 'contract'. Contracts between the Service Provider and other third parties are often (incorrectly) called SLAs, as the level of service has been set by the (principal) customer there can be no 'agreement' between third parties (these agreements are simply a 'contract'). Operating Level Agreements or OLA(s) however, may be used by internal groups to support SLA (s).
AnswerB is incorrect. Release Policy is a set of rules for deploying releases into the live operational
environment, defining different approaches for releases depending on their urgency and impact.
AnswerC is incorrect. The Service Level Requirements document contains the requirements for a service from the client viewpoint, defining detailed service level targets, mutual responsibilities, and other requirements specific to a certain group of customers. Answer D is incorrect.
Underpinning Contract (UC) is a contract between an IT service provider and a third party. In another way, it is an agreement between the IT organization and an external provider about the delivery of one or more services. The third party provides services that support the delivery of a service to a customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level targets in an SLA.

NEW QUESTION: 153
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: 154

Which of the following statements are true about declarative security? Each correct answer represents a complete solution. Choose all that apply.

A. It is employed in a layer that relies outside of the software code or uses attributes of the code.

B. It applies the security policies on the software applications at their runtime.

C. In this security, authentication decisions are made based on the business logic.

D. In this security, the security decisions are based on explicit statements.

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

Explanation/Reference:

Explanation: Declarative security applies the security policies on the software applications at their runtime.

In this type of security, the security decisions are based on explicit statements that confine security behavior. Declarative security applies security permissions that are required for the software application to access the local resources and provides role-based access control to an individual software component and software application. It is employed in a layer that relies outside of the software code or uses attributes of the code. AnswerC is incorrect. In declarative security, authentication decisions are coarse-grained in nature from an operational or external security perspective.

NEW QUESTION: 155

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: 156

Which of the following life cycle modeling activities establishes service relationships and message exchange paths?

A. Service-oriented logical design modeling

B. Service-oriented conceptual architecture modeling

C. Service-oriented discovery and analysis modeling

D. Service-oriented business integration modeling

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Explanation: The service-oriented logical design modeling establishes service relationships and message exchange paths. It also addresses service visibility and crafts service logical compositions.

NEW QUESTION: 157
Which of the following describes a residual risk as the risk remaining after a risk mitigation has occurred?
A. DIACAP
B. SSAA
C. DAA
D. ISSO
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation: DIACAP describes a residual risk as the risk remaining after a risk mitigation has occurred.
The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk. DIACAP replaced the former process, known as DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process), in 2006. DoD Instruction (DoDI) 8510.01 establishes a standard DoD-wide process with a set of activities, general tasks, and a management structure to certify and accredit an Automated Information System (AIS) that will maintain the Information Assurance (IA) posture of the Defense Information Infrastructure (DII) throughout the system's life cycle.DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. It identifies four phases: 1.System Definition
2.Verification 3.Validation 4.Re-Accreditation AnswerD 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. AnswerC is incorrect. The Designated Approving Authority (DAA), in the United States Department of Defense, is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. The DAA is responsible for implementing system security. The DAA can grant the accreditation and can determine that the system's risks are not at an acceptable level and the system is not ready to be operational. AnswerB 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.

NEW QUESTION: 158
In which of the following DIACAP phases is residual risk analyzed?
A. Phase 1
B. Phase 5
C. Phase 2
D. Phase 4
E. Phase 3
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation: The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk. The Certification Determination and Accreditation phase is the third phase in the DIACAP process. Its subordinate tasks are as follows: Analyze residual risk. Issue certification determination. Make accreditation decision. AnswerA is incorrect. Phase 1 is known as Initiate and Plan IA C&A. Answer: C is incorrect. Phase 2 is used to implement and validate assigned IA controls. Answer: E is incorrect. Phase 3 is used to make certification determination and accreditation decisions. Answer: B is incorrect. Phase 5 is known as decommission system and is used to conduct activities related to the disposition of the system data and objects.

NEW QUESTION: 159
In which type of access control do user ID and password system come under?
A. Physical
B. Technical
C. Power
D. Administrative
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: Technical access controls include IDS systems, encryption, network segmentation, and antivirus controls. AnswerD is incorrect. The policies and procedures implemented by an organization come under administrative access controls. AnswerA is incorrect. Security guards, locks on the gates, and alarms come under physical access controls. AnswerC is incorrect. There is no such type of access control as power control.

NEW QUESTION: 160

You work as a system engineer for BlueWell Inc. You want to verify that the build meets its data requirements, and correctly generates each expected display and report. Which of the following tests will help you to perform the above task?

A. Performance test

B. Functional test

C. Reliability test

D. Regression test

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Explanation: 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: 161

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

A. Principle of separation of privileges, duties, and roles

B. Assume environment data is not trustworthy

C. Simplify the design

D. Principle of least privilege

Answer: (SHOW ANSWER)

General Principle 1- Minimize the number of high-consequence targets includes the following principles and practices: Principle of least privilege Principle of separation of privileges, duties, and roles Principle of separation of domains Answer B is incorrect. Assume environment data is not trustworthy principle is included in the General Principle 2. Answer C is incorrect. Simplify the design principle is included in the General Principle 3.

NEW QUESTION: 162

According to the NIST SAMATE, dynamic analysis tools operate by generating runtime vulnerability scenario using some functions. Which of the following are functions that are used by the dynamic analysis tools and are summarized in the NIST SAMATE? Each correct answer represents a complete solution. Choose all that apply.

A. Implementation attack

B. Source code security

C. File corruption

D. Network fault injection

Answer: (SHOW ANSWER)

According to the NIST SAMATE, dynamic analysis tools operate by generating runtime vulnerability scenario using the following functions: Resource fault injection Network fault injection System fault injection User interface fault injection Design attack Implementation attack File corruption Answer B is incorrect. This function is summarized for static analysis tools.

NEW QUESTION: 163

Which of the following NIST documents provides a guideline for identifying an information system as a National Security System?

A. NIST SP 800-37

B. NIST SP 800-59

C. NIST SP 800-53

D. NIST SP 800-60

E. NIST SP 800-53A

Answer: (SHOW ANSWER)

NIST has developed a suite of documents for conducting Certification & Accreditation (C&A). These documents are as follows: NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems. NIST Special Publication 800-53: This document provides a guideline for security controls for Federal Information Systems. NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System. NIST Special Publication 800-59: This document is a guideline for identifying an information system as a National Security System. 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: 164

In 2003, NIST developed a new Certification & Accreditation (C&A) guideline known as FIPS 199. What levels of potential impact are defined by FIPS 199? Each correct answer represents a complete solution.

Choose all that apply.

A. Moderate

B. Medium

C. High

D. Low

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

Explanation/Reference:

Explanation: In 2003, NIST developed a new Certification & Accreditation (C&A) guideline known as FIPS

199. FIPS 199 is a standard for security categorization of Federal Information and Information Systems. It defines three levels of potential impact: Low: It causes a limited adverse effect. Medium: It causes a serious adverse effect. High: It causes a severe adverse effect.

NEW QUESTION: 165
In which of the following testing methods is the test engineer equipped with the knowledge of system and designs test cases or test data based on system knowledge?
A. Integration testing
B. Regression testing
C. Whitebox testing
D. Graybox testing
Answer: (SHOW ANSWER)
Graybox testing is a combination of whitebox testing and blackbox testing. In graybox testing, the test engineer is equipped with the knowledge of system and designs test cases or test data based on system knowledge. The security tester typically performs graybox testing to find vulnerabilities in software and network system. Answer C is incorrect. Whitebox testing is a testing technique in which an organization provides full knowledge about the infrastructure to the testing team. The information, provided by the organization, often includes network diagrams, source codes, and IP addressing information of the infrastructure to be tested. 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 B is incorrect. 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.

NEW QUESTION: 166
DRAG DROP
Drag and drop the appropriate external constructs in front of their respective functions.
Answer:
Explanation:
There are two types of compositional constructs: 1.External constructs: The various types of external constructs are as follows: Cascading: In this type of external construct, one system gains the input from the output of another system. Feedback: In this type of external construct, one system provides the input to another system, which in turn feeds back to the input of the first system. Hookup: In this type of external construct, one system communicates with another

system as well as with external entities. 2.Internal constructs: The internal constructs include intersection, union, and difference.

NEW QUESTION: 167
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)
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. Answer D 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. Answer B is incorrect. Availability means that data must be available whenever it is needed. Answer C 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: 168
An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?
A. Backup policy

B. User password policy
C. Privacy policy
D. Network security policy
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: Monitoring the computer hard disks or e-mails of employees pertains to the privacy policy of an organization. AnswerA is incorrect. The backup policy of a company is related to the backup of its data. Answer D is incorrect. The network security policy is related to the security of a company's network.
AnswerB is incorrect. The user password policy is related to passwords that users provide to log on to the
network.

NEW QUESTION: 169
You are the project manager of the GHY project for your organization. You are about to start the qualitative risk analysis process for the project and you need to determine the roles and responsibilities for conducting risk management. Where can you find this information?
A. Risk register
B. Staffing management plan
C. Risk management plan
D. Enterprise environmental factors
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: The risk management plan defines the roles and responsibilities for conducting risk management. A Risk management plan is a document arranged by a project manager to estimate the effectiveness, predict risks, and build response plans to mitigate them. It also consists of the risk assessment matrix. Risks are built in with any project, and project managers evaluate risks repeatedly and build plans to address them. The risk management plan consists of analysis of possible risks with both high and low impacts, and the mitigation strategies to facilitate the project and avoid being derailed through which the common problems arise. Risk management plans should be timely reviewed by the project team in order to avoid having the analysis become stale and not reflective of actual potential project risks. Most critically, risk management plans include a risk strategy for project execution. AnswerA is incorrect. The risk register does not define the risk management roles and responsibilities. AnswerD is incorrect.
Enterprise environmental factors may define the roles that risk management officials or departments play in the project, but the best answer for all projects is the risk management plan.
AnswerB is incorrect. The staffing management plan does not define the risk management roles and responsibilities.

NEW QUESTION: 170

The organization level is the Tier 1 and it addresses risks from an organizational perspective.
What are the various Tier 1 activities? Each correct answer represents a complete solution. Choose all that apply.
A. The organization plans to use the degree and type of oversight, to ensure that the risk management strategy is being effectively carried out.
B. The level of risk tolerance.
C. The techniques and methodologies an organization plans to employ, to evaluate information system- related security risks.
D. The RMF primarily operates at Tier 1.
Answer: A,B,C (LEAVE A REPLY)
Explanation/Reference:
Explanation: The Organization Level is the Tier 1, and it addresses risks from an organizational perspective. It includes the following points: The techniques and methodologies an organization plans to employ, to evaluate information system-related security risks. During risk assessment, the methods and procedures the organization plans to use, to evaluate the significance of the risks identified. The types and extent of risk mitigation measures the organization plans to employ, to address identified risks. The level of risk tolerance. According to the environment of operation, how the organization plans to monitor risks on an ongoing basis, given the inevitable changes to organizational information system.
The organization plans to use the degree and type of oversight, in order to ensure that the risk management strategy is being effectively carried out.Answer: D is incorrect. The RMF primarily operates at Tier 3.

NEW QUESTION: 171
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)
Explanation/Reference:
Explanation: 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. AnswerA is incorrect. It is not one of the primary functions of configuration management. It is the function of risk avoidance.

NEW QUESTION: 172

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

A. Certification and accreditation decision

B. Continue to review and refine the SSAA

C. Perform certification evaluation of the integrated system

D. System development

E. Develop recommendation to the DAA

Answer: A,B,C,E (LEAVE A REPLY)

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

NEW QUESTION: 173

DRAG DROP

Security code review identifies the unvalidated input calls made by an attacker and avoids those calls to be processed by the server. It performs various review checks on the stained calls of servlet for identifying unvalidated input from the attacker. Choose the appropriate review checks and drop them in front of their respective functions.

Answer:

The various security code review checks performed on the stained calls of servlet are as follows: getParameter(): It is used to check the unvalidated sources of input from URL parameters in javax.servlet.HttpServletRequest class. getQueryString(): It is used to check the unvalidated sources of input from Form fields in javax.servlet.HttpServletRequest class. getCookies(): It is used to check the unvalidated sources of input from Cookies javax.servlet.HttpServletRequest class. getHeaders(): It is used to check the unvalidated sources of input from HTTP headers javax.servlet.HttpServletRequest class.

NEW QUESTION: 174

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

A. Take-Grant Protection Model

B. Biba Integrity Model

C. Bell-LaPadula Model

D. Access Matrix

Answer: A (LEAVE A REPLY)

Explanation/Reference:

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

NEW QUESTION: 175
Which of the following are the tasks performed by the owner in the information classification schemes?
Each correct answer represents a part of the solution. Choose three.
A. To make original determination to decide what level of classification the information requires, which is based on the business requirements for the safety of the data.
B. To review the classification assignments from time to time and make alterations as the business requirements alter.
C. To perform data restoration from the backups whenever required.
D. To delegate the responsibility of the data safeguard duties to the custodian.
Answer: A,B,D (LEAVE A REPLY)
Explanation/Reference:
Explanation: The different tasks performed by the owner are as follows: He makes the original determination to decide what level of classification the information requires, which is based on the business requirements for the safety of the data. He reviews the classification assignments from time to time and makes alterations as the business needs change. He delegates the responsibility of the data safeguard duties to the custodian. He specifies controls to ensure confidentiality, integrity and availability.
AnswerC is incorrect. This task is performed by the custodian and not by the owner.

NEW QUESTION: 176
Which of the following security issues does the Bell-La Padula model focus on?
A. Authorization
B. Confidentiality
C. Integrity
D. Authentication
Answer: B (LEAVE A REPLY)

The Bell-La Padula model is a state machine model used for enforcing access control in large organizations. It focuses on data confidentiality and access to classified information, in contrast to the Biba Integrity model, which describes rules for the protection of data integrity. In the Bell-La Padula model, the entities in an information system are divided into subjects and objects. The Bell-La Padula model is built on the concept of a state machine with a set of allowable states in a computer network system. The transition from one state to another state is defined by transition functions. The model defines two mandatory access control (MAC) rules and one discretionary access control (DAC) rule with three security properties: 1.The Simple Security Property: A subject at a given security level may not read an object at a higher security level (no read-up). 2.The *-property (star-property): A subject at a given security level must not write to any object at a lower security level (no write-down). The *-property is also known as the Confinement property. 3.The Discretionary Security Property: It uses an access matrix to specify the discretionary access control.

NEW QUESTION: 177
A service provider guarantees for end-to-end network traffic performance to a customer. Which of the following types of agreement is this?
A. SLA
B. VPN
C. NDA
D. LA
Answer: A (LEAVE A REPLY)
This is a type of service-level agreement. A service-level agreement (SLA) is a negotiated agreement between two parties where one is the customer and the other is the service provider. It records a common understanding about services, priorities, responsibilities, guarantees, and warranties. Each area of service scope should have the 'level of service' defined. The SLA may specify the levels of availability, serviceability, performance, operation, or other attributes of the service, such as billing. Answer C is incorrect. Non-disclosure agreements (NDAs) are often used to protect the confidentiality of an invention as it is being evaluated by potential licensees. Answer D is incorrect. License agreements (LA) describe the rights and responsibilities of a party related to the use and exploitation of intellectual property. Answer B is incorrect. There is no such type of agreement as VPN.

NEW QUESTION: 178
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: (SHOW ANSWER)

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: 179

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. What are the process activities of this phase? Each correct answer represents a complete solution. Choose all that apply.

A. Certification analysis

B. Assessment of the Analysis Results

C. Configuring refinement of the SSAA

D. System development

E. Registration

Answer: A,B,C,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. The process activities of this phase are as follows: Configuring refinement of the SSAA System development Certification analysis Assessment of the Analysis Results Answer E is incorrect. Registration is a Phase 1 activity.

NEW QUESTION: 180

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

A. Security education

B. Security organization

C. System classification

D. Information classification

Answer: (SHOW ANSWER)

The first action of a management program to implement information security is to have a security program in place. The objectives of a security program are as follows: Protect the company and its assets Manage risks by identifying assets, discovering threats, and estimating the risk Provide direction for security activities by framing of information security policies, procedures, standards,

guidelines and baselines Information classification Security organization Security education Answer C is incorrect. System classification is not one of the objectives of a security program.

NEW QUESTION: 181
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)
Explanation/Reference:
Explanation: 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. AnswerB, D, and A are incorrect. These are invalid options.

NEW QUESTION: 182
Which of the following is NOT a responsibility of a data owner?
A. Approving access requests
B. Ensuring that the necessary security controls are in place
C. Delegating responsibility of the day-to-day maintenance of the data protection mechanisms to the data custodian
D. Maintaining and protecting data
Answer: D (LEAVE A REPLY)
Explanation/Reference:

Explanation: It is not a responsibility of a data owner. The data custodian (information custodian) is responsible for maintaining and protecting the data.
AnswerB, A, and C are incorrect. All of these are responsibilities of a data owner. The roles and responsibilities of a data owner are as follows: The data owner (information owner) is usually a member of management, in charge of a specific business unit, and is ultimately responsible for the protection and use of a specific subset of information. The data owner decides upon the classification of the data that he is responsible for and alters that classification if the business needs arise. This person is also responsible for ensuring that the necessary security controls are in place, ensuring that proper access rights are being used, defining security requirements per classification and backup requirements, approving any disclosure activities, and defining user access criteria. The data owner approves access requests or may choose to delegate this function to business unit managers. And it is the data owner who will deal with security violations pertaining to the data he is responsible for protecting. The data owner, who obviously has enough on his plate, delegates responsibility of the day-to-day maintenance of the data protection mechanisms to the data custodian.

NEW QUESTION: 183
Which of the following describes a residual risk as the risk remaining after a risk mitigation has occurred?
A. DIACAP
B. SSAA
C. DAA
D. ISSO
Answer: A (LEAVE A REPLY)
DIACAP describes a residual risk as the risk remaining after a risk mitigation has occurred. The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk. DIACAP replaced the former process, known as DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process), in 2006. DoD Instruction (DoDI) 8510.01 establishes a standard DoD-wide process with a set of activities, general tasks, and a management structure to certify and accredit an Automated Information System (AIS) that will maintain the Information Assurance (IA) posture of the Defense Information Infrastructure (DII) throughout the system's life cycle.DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. It identifies four phases: 1.System Definition 2.Verification 3.Validation 4.Re-Accreditation Answer D 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 C is incorrect. The Designated Approving Authority (DAA), in the United States Department of Defense, is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. The DAA is responsible for implementing system security. The DAA can grant the accreditation and can determine that the system's risks are not at an acceptable level and the system is not ready to be operational. Answer B 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.

NEW QUESTION: 184
You work as a security engineer for BlueWell Inc. Which of the following documents will you use as a guide for the security certification and accreditation of Federal Information Systems?
A. NIST Special Publication 800-60
B. NIST Special Publication 800-53
C. NIST Special Publication 800-37
D. NIST Special Publication 800-59
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: NIST has developed a suite of documents for conducting Certification & Accreditation (C&A).
These documents are as follows: NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems.
NIST Special Publication 800-53: This document provides a guideline for security controls for Federal Information Systems. NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System. NIST Special Publication 800-59: This document is a guideline for identifying an information system as a National Security System. 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: 185
At which of the following levels of robustness in DRM must the security functions be immune to widely available tools and specialized tools and resistant to professional tools?
A. Level 2
B. Level 4
C. Level 1
D. Level 3

Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation: At Level 1 of robustness in DRM, the security functions must be immune to widely available tools and specialized tools and resistant to professional tools.

NEW QUESTION: 186
Which of the following types of obfuscation transformation increases the difficulty for a de-obfuscation tool so that it cannot extract the true application from the obfuscated version?
A. Preventive transformation
B. Data obfuscation
C. Control obfuscation
D. Layout obfuscation
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation: Preventive transformation increases the difficulty for a de-obfuscation tool so that it cannot extract the true application from the obfuscated version.

NEW QUESTION: 187
Which of the following penetration testing techniques automatically tests every phone line in an exchange and tries to locate modems that are attached to the network?
A. Demon dialing
B. Sniffing
C. Social engineering
D. Dumpster diving
Answer: (SHOW ANSWER)
The demon dialing technique automatically tests every phone line in an exchange and tries to locate modems that are attached to the network. Information about these modems can then be used to attempt external unauthorized access. Answer B is incorrect. In sniffing, a protocol analyzer is used to capture data packets that are later decoded to collect information such as passwords or infrastructure configurations. Answer D is incorrect. Dumpster diving technique is used for searching paper disposal areas for unshredded or otherwise improperly disposed-of reports. Answer C is incorrect. Social engineering is the most commonly used technique of all, getting information (like passwords) just by asking for them.

NEW QUESTION: 188
Harry is the project manager of the MMQ Construction Project. In this project, Harry has identified a supplier who can create stained glass windows for 1,000 window units in the construction project. The supplier is an artist who works by himself, but creates windows for several companies throughout the United States. Management reviews the proposal to use this supplier and while they agree that the supplier is talented, they do not think the artist can fulfill the 1,000 window units in time for the project's deadline. Management asked Harry to find a supplier who

can fulfill the completion of the windows by the needed date in the schedule. What risk response has management asked Harry to implement?

A. Transference

B. Avoidance

C. Mitigation

D. Acceptance

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation: This is an example of mitigation. By changing to a more reliable supplier, Harry is reducing the probability the supplier will be late. It's still possible that the vendor may not be able to deliver the stained glass windows, but the more reputable supplier reduces the probability of the lateness. Mitigation is a risk response planning technique associated with threats that seeks to reduce the probability of occurrence or impact of a risk to below an acceptable threshold. Risk mitigation involves taking early action to reduce the probability and impact of a risk occurring on the project. Adopting less complex processes, conducting more tests, or choosing a more stable supplier are examples of mitigation actions.

AnswerA is incorrect. Transference is when the risk is transferred to a third party, usually for a fee. While

this question does include a contractual relationship, the risk is the lateness of the windows. Transference focuses on transferring the risk to a third party to manage the risk event. In this instance, the management of the risk is owned by a third party; the third party actually creates the risk event because of the possibility of the lateness of the windows. AnswerB is incorrect. Avoidance changes the project plan to avoid the risk. If the project manager and management changed the window-type to a standard window in the project requirements, then this would be avoidance. Risk avoidance is a technique used for threats. It creates changes to the project management plan that are meant to either eliminate the risk completely or to protect the project objectives from its impact. Risk avoidance removes the risk event entirely either by adding additional steps to avoid the event or reducing the project scope requirements. It may seem the answer to all possible risks, but avoiding risks also means losing out on the potential gains that accepting (retaining) the risk might have allowed. AnswerD is incorrect. Acceptance accepts the risk that the windows could be late and offers no response.

NEW QUESTION: 189

Which of the following statements about the availability concept of Information security management is true?

A. It ensures that modifications are not made to data by unauthorized personnel or processes.

B. It determines actions and behaviors of a single individual within a system.

C. It ensures reliable and timely access to resources.

D. It ensures that unauthorized modifications are not made to data by authorized personnel or processes.

Answer: C (LEAVE A REPLY)

The concept of availability ensures reliable and timely access to data or resources. In other words, availability ensures that the systems are up and running when needed. The availability concept also ensures that the security services are in working order. Answer A and D are incorrect. The concept of integrity ensures that modifications are not made to data by unauthorized personnel or processes. It also ensures that unauthorized modifications are not made to data by authorized personnel or processes. Answer B is incorrect. Accountability determines the actions and behaviors of an individual within a system, and identifies that particular individual. Audit trails and logs support accountability.

NEW QUESTION: 190
Which of the following actions does the Data Loss Prevention (DLP) technology take when an agent detects a policy violation for data of all states? Each correct answer represents a complete solution. Choose all that apply.
A. It creates an alert.
B. It quarantines the file to a secure location.
C. It reconstructs the session.
D. It blocks the transmission of content.
Answer: (SHOW ANSWER)
When an agent detects a policy violation for data of all states, the Data Loss prevention (DLP) technology takes one of the following actions: It creates an alert. It notifies an administrator of a violation. It quarantines the file to a secure location. It encrypts the file. It blocks the transmission of content. Answer C is incorrect. Data Loss Prevention (DLP) reconstructs the session when data is in motion.

NEW QUESTION: 191
Security is a state of well-being of information and infrastructures in which the possibilities of successful yet undetected theft, tampering, and/or disruption of information and services are kept low or tolerable. Which of the following are the elements of security? Each correct answer represents a complete solution. Choose all that apply.
A. Integrity
B. Authenticity
C. Confidentiality
D. Availability
Answer: A,B,C,D (LEAVE A REPLY)
The elements of security are as follows: 1.Confidentiality: It is the concealment of information or resources. 2.Authenticity: It is the identification and assurance of the origin of information. 3.Integrity: It refers to the trustworthiness of data or resources in terms of preventing improper and unauthorized changes. 4.Availability: It refers to the ability to use the information or resources as desired.

NEW QUESTION: 192

You are advising a school district on disaster recovery plans. In case a disaster affects the main IT centers for the district they will need to be able to work from an alternate location. However, budget is an issue. Which of the following is most appropriate for this client?

A. Cold site

B. Off site

C. Warm site

D. Hot site

Answer: A (LEAVE A REPLY)

A cold site provides an office space, and in some cases basic equipment. However, you will need to restore your data to that equipment in order to use it. This is a much less expensive solution than the hot site. Answer D is incorrect. A hot site has equipment installed, configured and ready to use. This may make disaster recovery much faster, but will also be more expensive. And a school district can afford to be down for several hours before resuming IT operations, so the less expensive option is more appropriate. Answer C is incorrect. A warm site is between a hot and cold site. It has some equipment ready and connectivity ready. However, it is still significantly more expensive than a cold site, and not necessary for this scenario. Answer B is incorrect. Off site is not any type of backup site terminology.

NEW QUESTION: 193

Which of the following plans is documented and organized for emergency response, backup operations, and recovery maintained by an activity as part of its security program that will ensure the availability of critical resources and facilitates the continuity of operations in an emergency situation?

A. Continuity Of Operations Plan

B. Business Continuity Plan

C. Contingency Plan

D. Disaster Recovery Plan

Answer: C (LEAVE A REPLY)

Contingency plan is prepared and documented for emergency response, backup operations, and recovery maintained by an activity as the element of its security program that will ensure the availability of critical resources and facilitates the continuity of operations in an emergency situation. A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. 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. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption. Answer D is incorrect. A disaster recovery plan should contain data, hardware, and software that can be critical for a business. It should also include the plan for sudden loss such as hard disc crash. The business should use backup and data recovery utilities to limit the loss of data. Answer A is

incorrect. The Continuity Of Operation Plan (COOP) refers to the preparations and institutions maintained by the United States government, providing survival of federal government operations in the case of catastrophic events. It provides procedures and capabilities to sustain an organization's essential. COOP is the procedure documented to ensure persistent critical operations throughout any period where normal operations are unattainable. Answer B is incorrect. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan.

NEW QUESTION: 194
Which of the following agencies is responsible for funding the development of many technologies such as computer networking, as well as NLS?
A. DIAP
B. DTIC
C. DARPA
D. DISA
Answer: (SHOW ANSWER)
The Defense Advanced Research Projects Agency (DARPA) is an agency of the United States Department of Defense responsible for the development of new technology for use by the military. DARPA has been responsible for funding the development of many technologies which have had a major effect on the world, including computer networking, as well as NLS, which was both the first hypertext system, and an important precursor to the contemporary ubiquitous graphical user interface. DARPA supplies technological options for the entire Department, and is designed to be the "technological engine" for transforming DoD. Answer D is incorrect. The Defense Information Systems Agency is a United States Department of Defense combat support agency with the goal of providing real-time information technology (IT) and communications support to the President, Vice President, Secretary of Defense, the military Services, and the Combatant Commands. DISA, a Combat Support Agency, engineers and provides command and control capabilities and enterprise infrastructure to continuously operate and assure a global net-centric enterprise in direct support to joint warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations. Answer B is incorrect. The Defense Technical Information Center (DTIC) is a repository of scientific and technical documents for the United States Department of Defense. DTIC serves the DoD community as the largest central resource for DoD and government-funded scientific, technical, engineering, and business related information available today. DTIC's documents are available to DoD personnel and defense contractors, with unclassified documents also available to the public. DTIC's aim is to serve a vital link in the transfer of information among DoD personnel, DoD contractors, and potential contractors and other U.S. Government agency personnel and their contractors. Answer A is incorrect. The Defense-wide Information Assurance Program (DIAP) protects and supports DoD information, information systems, and information networks, which is important to the Department and the

armed forces throughout the day-to-day operations, and in the time of crisis. The DIAP uses the OSD method to plan, observe, organize, and incorporate IA activities. The role of DIAP is to act as a facilitator for program execution by the combatant commanders, Military Services, and Defense Agencies. The DIAP staff combines functional and programmatic skills for a comprehensive Defense-wide approach to IA. The DIAP's main objective is to ensure that the DoD's vital information resources are secured and protected by incorporating IA activities to get a secure net-centric GIG operation enablement and information supremacy by applying a Defense-in-Depth methodology that integrates the capabilities of people, operations, and technology to establish a multi-layer, multidimensional protection.