ISC2

Exam Questions CSSLP

Certified Information Systems Security Professional

NEW QUESTION 1
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

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 2
Which of the following are the common roles with regard to data in an information classification program? Each correct answer represents a complete solution. Choose all that apply.

A. Editor
B. Custodian
C. Owner
D. User
E. Security auditor

Answer: BCDE

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

NEW QUESTION 3
Joseph works as a Software Developer for WebTech Inc. He wants to protect the algorithms and the techniques of programming that he uses in developing an application. Which of the following laws are used to protect a part of software?

A. Code Security law
B. Patent laws
C. Trademark laws
D. Copyright laws

Answer: B

Explanation:
Patent laws are used to protect the duplication of software. Software patents cover the algorithms and techniques that are used in creating the software. It does not cover the entire program of the software. Patents give the author the right to make and sell his product. The time of the patent of a product is limited though, i.e., the author of the product has the right to use the patent for only a specific length of time. Answer D is incorrect. Copyright laws protect original works or creations of authorship including literary, dramatic, musical, artistic, and certain other intellectual works.

NEW QUESTION 4
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: ABC

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 5
In which of the following types of tests are the disaster recovery checklists distributed to the members of disaster recovery team and asked to review the assigned checklist?

A. Parallel test
B. Simulation test
C. Full-interruption test
D. Checklist test

Answer: D

Explanation:
A checklist test is a test in which the disaster recovery checklists are distributed to the members of the disaster recovery team. All members are asked to review the assigned checklist. The checklist test is a simple test and it is easy to conduct this test. It allows to accomplish the following three goals: It ensures that the employees are aware of their responsibilities and they have the refreshed knowledge. It provides an individual with an opportunity to review the checklists for obsolete information and update any items that require modification during the changes in the organization. It ensures that the assigned members of disaster recovery team are still working for the organization. Answer B is incorrect. 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. 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. Answer C 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.

NEW QUESTION 6
Which of the following is an example of over-the-air (OTA) provisioning in digital rights management?

A. Use of shared secrets to initiate or rebuild trust.
B. Use of software to meet the deployment goals.
C. Use of concealment to avoid tampering attacks.
D. Use of device properties for unique identification.

Answer: A

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

NEW QUESTION 7
Which of the following types of redundancy prevents attacks in which an attacker can get physical control of a machine, insert unauthorized software, and alter data?

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

Answer: C

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

NEW QUESTION 8
Which of the following cryptographic system services ensures that information will not be disclosed to any unauthorized person on a local network?

A. Authentication
B. Integrity
C. Non-repudiation
D. Confidentiality

Answer: D

Explanation:
The confidentiality service of a cryptographic system ensures that information will not be disclosed to any unauthorized person on a local network.

NEW QUESTION 9
You work as a project manager for BlueWell Inc. You are working on a project and the management wants a rapid and cost-effective means for establishing priorities for planning risk responses in your project. Which risk management process can satisfy management's objective for your project?

A. Qualitative risk analysis
B. Historical information
C. Rolling wave planning
D. Quantitative analysis

Answer: A

Explanation:
Qualitative risk analysis is the best answer as it is a fast and low-cost approach to analyze the risk impact and its effect. It can promote certain risks onto risk response planning. Qualitative Risk Analysis uses the likelihood and impact of the identified risks in a fast and cost-effective manner. Qualitative Risk Analysis establishes a basis for a focused quantitative analysis or Risk Response Plan by evaluating the precedence of risks with a concern to impact on the project's scope, cost, schedule, and quality objectives. The qualitative risk analysis is conducted at any point in a project life cycle. The primary goal of qualitative risk analysis is to determine proportion of effect and theoretical response. The inputs to the Qualitative Risk Analysis process are: Organizational process assets Project Scope Statement Risk Management Plan Risk Register Answer B is incorrect. Historical information can be helpful in the qualitative risk analysis, but it is not the best answer for the question as historical information is not always available (consider new projects). Answer D is incorrect. Quantitative risk analysis is in-depth and often requires a schedule and budget for the analysis. Answer C is incorrect. Rolling wave planning is not a valid answer for risk analysis processes.

NEW QUESTION 10
Which of the following methods determines the principle name of the current user and returns the jav a.security.Principal object in the HttpServletRequest interface?

A. getUserPrincipal()
B. isUserInRole()
C. getRemoteUser()
D. getCallerPrincipal()

Answer: A

Explanation:
The getUserPrincipal() method determines the principle name of the current user and returns the java.security.Principal object. The java.security.Principal object contains the remote user name. The value of the getUserPrincipal() method returns null if no user is authenticated. Answer C is incorrect. The getRemoteUser() method returns the user name that is used for the client authentication. The value of the getRemoteUser() method returns null if no user is authenticated. Answer B is incorrect. The isUserInRole() method determines whether the remote user is granted a specified user role. The value of the isUserInRole() method returns true if the remote user is granted the specified user role;
otherwise it returns false. Answer D is incorrect. The getCallerPrincipal() method is used to identify a caller using a java.security.Principal object. It is not used in the HttpServletRequest interface.

NEW QUESTION 10
Which of the following organizations assists the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies?

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

Answer: A

Explanation:
The Office of Management and Budget (OMB) is a Cabinet-level office, and is the largest office within the Executive Office of the President (EOP) of the United States. The current OMB Director is Peter Orszag and was appointed by President Barack Obama. The OMB's predominant mission is to assist the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies. In helping to formulate the President's spending plans, the OMB evaluates the effectiveness of agency programs, policies, and procedures, assesses competing funding demands among agencies, and sets funding priorities. The OMB ensures that agency reports, rules, testimony, and proposed legislation are consistent with the President's Budget and with Administration policies.
Answer D is incorrect. The DCAA has the aim to monitor contractor costs and perform contractor audits. Answer C is incorrect. The National Security Agency/Central Security Service (NSA/CSS) is a crypto-logic intelligence agency of the United States government. It is administered as part of the United States Department of Defense. NSA is responsible for the collection and analysis of foreign communications and foreign signals intelligence, which involves cryptanalysis. NSA is also responsible for protecting U.S. government communications and information systems from similar agencies elsewhere, which involves cryptography. NSA is a key component of the U.S. Intelligence Community, which is headed by the Director of National Intelligence. The Central Security Service is a co- located agency created to coordinate intelligence activities and co-operation between NSA and U.S. military cryptanalysis agencies. NSA's work is limited to communications intelligence. It does not perform field or human intelligence activities. Answer B is incorrect. The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.

NEW QUESTION 12
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. In order to do so, he performs the following steps of the pre-attack phase successfully: Information gathering Determination of network range Identification of active systems Location of open ports and applications Now, which of the following tasks should he perform next?

A. Perform OS fingerprinting on the We-are-secure network.
B. Map the network of We-are-secure Inc.
C. Install a backdoor to log in remotely on the We-are-secure server.
D. Fingerprint the services running on the we-are-secure network.

Answer: A

Explanation:
John will perform OS fingerprinting on the We-are-secure network. Fingerprinting is the easiest way to detect the Operating System (OS) of a remote system. OS

detection is important because, after knowing the target system's OS, it becomes easier to hack into the system. The comparison of data packets that are sent by the target system is done by fingerprinting. The analysis of data packets gives the attacker a hint as to which operating system is being used by the remote system. There are two types of fingerprinting techniques as follows: 1.Active fingerprinting 2.Passive fingerprinting In active fingerprinting ICMP messages are sent to the target system and the response message of the target system shows which OS is being used by the remote system. In passive fingerprinting the number of hops reveals the OS of the remote system. Answer D and B are incorrect. John should perform OS fingerprinting first, after which it will be easy to identify which services are running on the network since there are many services that run only on a specific operating system. After performing OS fingerprinting, John should perform networking mapping. Answer C is incorrect. This is a pre-attack phase, and only after gathering all relevant knowledge of a network should John install a backdoor.

NEW QUESTION 17
In which of the following cryptographic attacking techniques does an attacker obtain encrypted messages that have been encrypted using the same encryption algorithm?

A. Chosen plaintext attack
B. Chosen ciphertext attack
C. Ciphertext only attack
D. Known plaintext attack

Answer: C

Explanation:
In a ciphertext only attack, an attacker obtains encrypted messages that have been encrypted using the same encryption algorithm.

NEW QUESTION 19
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 statement
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: ABC

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 21
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: ABCE

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 22
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

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 24
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

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 27
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: ABC

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 28
Which of the following methods does the Java Servlet Specification v2.4 define in the HttpServletRequest interface that control programmatic security? Each correct answer represents a complete solution. Choose all that apply.

A. getCallerIdentity()
B. isUserInRole()
C. getUserPrincipal()
D. getRemoteUser()

Answer: BCD

Explanation:
The various methods of the HttpServletRequest interface are as follows: getRemoteUser(): It returns the user name that is used for the client authentication. The value of the getRemoteUser() method returns null if no user is authenticated. isUserInRole(): It determines whether the remote user is granted a specified user role. The value of the isUserInRole() method returns true if the remote user is granted the specified user role; otherwise it returns false. getUserPrincipal(): It determines the principle name of the current user and returns the java.security.Principal object. The java.security.Principal object contains the remote user name. The value of the getUserPrincipal() method returns null if no user is authenticated. Answer A is incorrect. It is not defined in the HttpServletRequest interface. The getCallerIdentity() method is used to obtain the java.security.Identity of the caller.

NEW QUESTION 32
Microsoft software security expert Michael Howard defines some heuristics for determining code review in "A Process for Performing Security Code Reviews". Which of the following heuristics increase the application's attack surface? Each correct answer represents a complete solution. Choose all that apply.

A. Code written in C/C++/assembly language
B. Code listening on a globally accessible network interface
C. Code that changes frequently
D. Anonymously accessible code
E. Code that runs by default
F. Code that runs in elevated context

Answer: BDEF

Explanation:
Microsoft software security expert Michael Howard defines the following heuristics for determining code review in "A Process for Performing Security Code Reviews": Old code: Newer code provides better understanding of software security and has lesser number of vulnerabilities. Older code must be checked deeply. Code that runs by default: It must have high quality, and must be checked deeply than code that does not execute by default. Code that runs by default increases the application's attack surface. Code that runs in elevated context: It must have higher quality. Code that runs in elevated privileges must be checked deeply and increases the application's attack surface. Anonymously accessible code: It must be checked deeply than code that only authorized users and administrators can access, and it increases the application's attack surface. Code listening on a globally accessible network interface: It must be checked deeply for security vulnerabilities and increases the application's attack surface. Code written in C/C++/assembly language: It is prone to security vulnerabilities, for example, buffer overruns. Code with a history of security vulnerabilities: It includes additional vulnerabilities except concerted efforts that are required for removing them. Code that

handles sensitive data: It must be checked deeply to ensure that data is protected from unintentional disclosure. Complex code: It includes undiscovered errors because it is more difficult to analyze complex code manually and programmatically. Code that changes frequently: It has more security vulnerabilities than code that does not change frequently.

NEW QUESTION 33
Which of the following are examples of the application programming interface (API)? Each correct answer represents a complete solution. Choose three.

A. HTML
B. PHP
C. .NET
D. Perl

Answer: BCD

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

NEW QUESTION 37
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

Explanation:
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 40
Which of the following attacks causes software to fail and prevents the intended users from accessing software?

A. Enabling attack
B. Reconnaissance attack
C. Sabotage attack
D. Disclosure attack

Answer: C

Explanation:
A sabotage attack is an attack that causes software to fail. It also prevents the intended users from accessing software. A sabotage attack is referred to as a denial of service (DoS) or compromise of availability. Answer B is incorrect. The reconnaissance attack enables an attacker to collect information about software and operating environment. Answer D is incorrect. The disclosure attack exposes the revealed data to an attacker. Answer A is incorrect. The enabling attack delivers an easy path for other attacks.

NEW QUESTION 43
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

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 45
The LeGrand Vulnerability-Oriented Risk Management method is based on vulnerability analysis and consists of four principle steps. Which of the following processes does the risk assessment step include? Each correct answer represents a part of the solution. Choose all that apply.

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

Answer: BCD

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

NEW QUESTION 49
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

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 51
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

Explanation:
A life cycle model helps to provide an insight into the development process and emphasizes on the relationships among the different activities in this process. This model describes a structured approach to the development and adjustment process involved in producing and maintaining systems. The life cycle model addresses specifications, design, requirements, verification and validation, and maintenance activities.

NEW QUESTION 53
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: C

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 54
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: ABD

Explanation:
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 58
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

Explanation:
A B-rated system of the orange book has mandatory protection of the trusted computing base (TCB).
Trusted computing base (TCB) refers to hardware, software, controls, and processes that cause a computer system or network to be devoid of malicious software or hardware. Maintaining the trusted computing base (TCB) is essential for security policy to be implemented successfully.

NEW QUESTION 61
You are the project manager for GHY Project and are working to create a risk response for a negative risk. You and the project team have identified the risk that the project may not complete on time, as required by the management, due to the creation of the user guide for the software you're creating. You have elected to hire an external writer in order to satisfy the requirements and to alleviate the risk event. What type of risk response have you elected to use in this instance?

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

Answer: A

Explanation:
This is an example of transference as you have transferred the risk to a third party. Transference almost always is done with a negative risk event and it usually requires a contractual relationship.

NEW QUESTION 64
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

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 66
The Project Risk Management knowledge area focuses on which of the following processes? Each correct answer represents a complete solution. Choose all that apply.

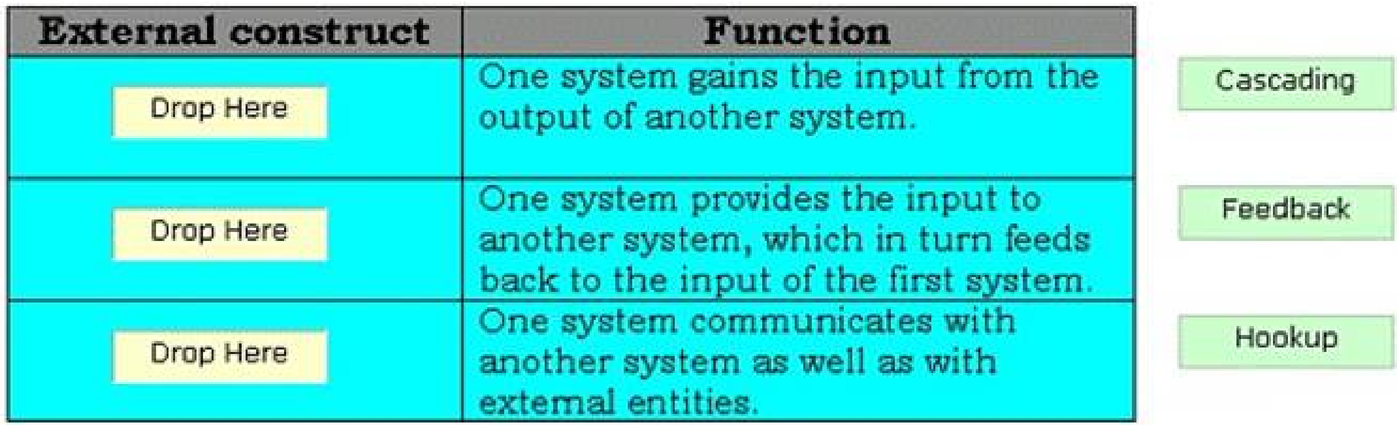
A. Risk Monitoring and Control
B. Risk Management Planning
C. Quantitative Risk Analysis
D. Potential Risk Monitoring

Answer: ABC

Explanation:
The Project Risk Management knowledge area focuses on the following processes: Risk Management Planning Risk Identification Qualitative Risk Analysis

Quantitative Risk Analysis Risk Response Planning Risk Monitoring and Control Answer D is incorrect. There is no such process in the Project Risk Management knowledge area.

NEW QUESTION 70
DRAG DROPDrag and drop the appropriate external constructs in front of their respective functions.



External construct	Function
Drop Here	One system gains the input from the output of another system.
Drop Here	One system provides the input to another system, which in turn feeds back to the input of the first system.
Drop Here	One system communicates with another system as well as with external entities.

Cascading

Feedback

Hookup

A. Mastered
B. Not Mastered

Answer: A

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 75
Which of the following techniques is used to identify attacks originating from a botnet?

A. Passive OS fingerprinting
B. Recipient filtering
C. IFilter
D. BPF-based filter

Answer: A

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

NEW QUESTION 76
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

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. Answer C is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected. Answer A is incorrect. Packet sniffing is a process of monitoring data packets that travel across a network. The software used for packet sniffing is known as sniffers. There are many packet-sniffing programs that are available on the Internet. Some of these are unauthorized, which can be harmful for a network's security.

NEW QUESTION 80
Which of the following techniques is used when a system performs the penetration testing with the objective of accessing unauthorized information residing inside a computer?

A. Biometrician
B. Van Eck Phreaking
C. Port scanning
D. Phreaking

Answer: C

Explanation:
Port scanning identifies open doors to a computer. Hackers and crackers use this technique to obtain unauthorized information.
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. Answer D is incorrect. Phreaking is a process used to crack the phone system. The main aim of phreaking is to avoid paying for long-distance calls. As telephone networks have become computerized, phreaking has become closely linked with computer hacking. This is sometimes called the H/P culture (with H standing for Hacking and P standing for Phreaking). Answer A is incorrect. It is defined as a system using a physical attribute for authenticating. Only authorized users are provided access to network or application. Answer B is incorrect. It is described as a form of eavesdropping in which special equipments are used to pick up the telecommunication signals or data within a computer device.

NEW QUESTION 84
Which of the following is an open source network intrusion detection system?

A. NETSH
B. Macof
C. Sourcefire
D. Snort

Answer: D

Explanation:
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. Macof is a tool of the dsniff tool set and used to flood the local network with random MAC addresses. It causes some switches to fail open in repeating mode, and facilitates sniffing. Answer C is incorrect. Sourcefire is the company that owns and maintains Snort. Answer A is incorrect. NETSH is not a network intrusion detection system. NETSH is a command line tool to configure TCP/IP settings such as the IP address, Subnet Mask, Default Gateway, DNS, WINS addresses, etc.

NEW QUESTION 89
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

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 90
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. What phases are identified by DIACAP? Each correct answer represents a complete solution. Choose all that apply.

A. System Definition
B. Validation
C. Identification
D. Accreditation
E. Verification
F. Re-Accreditation

Answer: ABEF

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. 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

NEW QUESTION 93
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

Explanation:
Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The C&A process is used extensively in the U.S. Federal Government. Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. 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 94
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

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 96
What are the various phases of the Software Assurance Acquisition process according to the U.S. Department of Defense (DoD) and Department of Homeland Security (DHS) Acquisition and Outsourcing Working Group?

A. Implementing, contracting, auditing, monitoring
B. Requirements, planning, monitoring, auditing
C. Planning, contracting, monitoring and acceptance, follow-on
D. Designing, implementing, contracting, monitoring

Answer: C

Explanation:
Software Assurance Acquisition process defines the level of confidence that software is free from vulnerabilities. It is designed into the software or accidentally inserted at anytime during its lifecycle, and the software works in a planned manner. According to the U.S. Department of Defense and Department of Homeland Security Acquisition and Outsourcing Working Group, the Software Assurance Acquisition process contains the following phases:
* 1.Planning 2.Contracting 3.Monitoring and acceptance 4.Follow-on

NEW QUESTION 101
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: B

Explanation:
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 B 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 105
Adrian is the project manager of the NHP Project. In her project there are several work packages that deal with electrical wiring. Rather than to manage the risk internally she has decided to hire a vendor to complete all work packages that deal with the electrical wiring. By removing the risk internally to a licensed electrician Adrian feels more comfortable with project team being safe. What type of risk response has Adrian used in this example?

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

Answer: D

Explanation:
This is an example of transference. When the risk is transferred to a third party, usually for a fee, it creates a contractual-relationship for the third party to manage the risk on behalf of the performing organization. Risk response planning is a method of developing options to decrease the amount of threats and make the most of opportunities. The risk response should be aligned with the consequence of the risk and cost- effectiveness. This planning documents the processes for managing risk events. It addresses the owners and their responsibilities, risk identification, results from qualification and quantification processes, budgets and times for responses, and contingency plans. The various risk response planning techniques are as follows: Risk acceptance: It indicates that the project team has decided not to change the project management plan to deal with a risk, or is unable to identify any other suitable response strategy. Risk avoidance: It is a technique for a threat, which creates changes to the project management plan that are meant to either eliminate the risk or to protect the project objectives from this impact. Risk mitigation: It is a list of specific actions being taken to deal with specific risks associated with the threats and seeks to reduce the probability of occurrence or impact of risk below an acceptable threshold. Risk transference: It is used to shift the impact of a threat to a third party, together with the ownership of the response.

NEW QUESTION 107
Which of the following specifies access privileges to a collection of resources by using the URL mapping?

A. Code Access Security
B. Security constraint
C. Configuration Management
D. Access Management

Answer: B

Explanation:
Security constraint is a type of declarative security, which specifies the protection of web content. It also specifies access privileges to a collection of resources by using the URL mapping. A deployment descriptor is used to define the security constraint. Security constraint includes the following elements: Web resource collection Authorization constraint User data constraint Answer A is incorrect. Code Access Security (CAS), in the Microsoft .NET framework, is Microsoft's solution to prevent untrusted code from performing privileged actions. When the CLR (common language runtime) loads an assembly it will obtain evidence for the assembly and use this to identify the code group that the assembly belongs to. A code group contains a permission set (one or more permissions). Code that performs a privileged action will perform a code access demand, which will cause the CLR to walk up the call stack and examine the permission set granted to the assembly of each method in the call stack. The code groups and permission sets are determined by the administrator of the machine who defines the security policy. Answer D is incorrect. Access Management is used to grant authorized users the right to use a service, while preventing access to non- authorized users. The Access Management process essentially executes policies defined in IT Security Management. It is sometimes also referred to as Rights Management or Identity Management. It is part of Service Operation and the owner of Access Management is the Access Manager. Access Management is added as a new process to ITIL V3. The sub-processes of Access Management are as follows: Maintain Catalogue of User Roles and Access Profiles Manage User Access Requests Answer B 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.

NEW QUESTION 109
The Web resource collection is a security constraint element summarized in the Java Servlet Specification v2.4. Which of the following elements does it include? Each correct answer represents a complete solution. Choose two.

A. HTTP methods
B. Role names
C. Transport guarantees
D. URL patterns

Answer: AD

Explanation:
Web resource collection is a set of URL patterns and HTTP operations that define all resources required to be protected. It is a security constraint element summarized in the Java Servlet Specification v2.4. The Web resource collection includes the following elements: URL patterns HTTP methods Answer B is incorrect. An authorization constraint includes role names. Answer B is incorrect. A user data constraint includes transport guarantees.

NEW QUESTION 113
Which of the following features of SIEM products is used in analysis for identifying potential problems and reviewing all available data that are associated with the problems?

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

Answer: B

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

NEW QUESTION 117
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

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

NEW QUESTION 121
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

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. Answer D is incorrect. Injection flaw occurs when data is sent to an interpreter as a part of command or query. Answer A is incorrect. Insecure cryptographic storage occurs when applications have failed to encrypt datAnswer B is incorrect. Insecure communication occurs when applications have failed to encrypt network traffic.

NEW QUESTION 124
An attacker exploits actual code of an application and uses a security hole to carry out an attack before the application vendor knows about the vulnerability. Which of the following types of attack is this?

A. Replay
B. Zero-day
C. Man-in-the-middle
D. Denial-of-Service

Answer: B

Explanation:
A zero-day attack, also known as zero-hour attack, is a computer threat that tries to exploit computer application vulnerabilities which are unknown to others, undisclosed to the software vendor, or for which no security fix is available. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software vendor knows about the vulnerability. User awareness training is the most effective technique to mitigate such attacks. Answer A is incorrect. A replay attack is a type of attack in which attackers capture packets containing passwords or digital signatures whenever packets pass between two hosts on a network. In an attempt to obtain an authenticated connection, the attackers then resend the captured packet to the system. In this type of attack, the attacker does not know the actual password, but can simply replay the captured packet. Answer B is incorrect. Man-in-the-middle attacks occur when an attacker successfully inserts an intermediary software or program between two communicating hosts. The intermediary software or program allows attackers to listen to and modify the communication packets passing between the two hosts. The software intercepts the communication packets and then sends the information to the receiving host. The receiving host responds to the software, presuming it to be the legitimate client. Answer D is incorrect. A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as network saturation attack or bandwidth consumption attack. Attackers perform DoS attacks by sending a large number of protocol packets to a network.

NEW QUESTION 127
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

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 129
Which of the following security models characterizes the rights of each subject with respect to every object in the computer system?

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

Answer: D

Explanation:
The access matrix or access control matrix is an abstract, formal security model of protection state in computer systems that characterizes the rights of each subject with respect to every object in the system. It was first introduced by Butler W. Lampson in 1971. According to the access matrix model, the protection state of a computer system can be abstracted as a set of objects 'O', that is the set of entities that needs to be protected (e.g. processes, files, memory pages) and a set of subjects 'S' that consists of all active entities (e.g. users, processes). Further there exists a set of rights 'R' of the form r(s,o), where s S, o O and r(s,o) R. A right thereby specifies the kind of access a subject is allowed to process with regard to an object. Answer B is incorrect. The Bell-La Padula Model is a state machine model used for enforcing access control in government and military applications. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g.,"Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public"). The Bell-La Padula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity. Answer A is incorrect. The Clark-Wilson model provides a foundation for specifying and analyzing an integrity policy for a computing system. The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. The model's enforcement and certification rules define data items and processes that provide the basis for an integrity policy. The core of the model is based on the notion of a transaction. Answer B is incorrect. The Biba model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject.

NEW QUESTION 130
Which of the following phases of the DITSCAP C&A process is used to define the C&A level of effort, to identify the main C&A roles and responsibilities, and to create an agreement on the method for implementing the security requirements?

A. Phase 1
B. Phase 4
C. Phase 2
D. Phase 3

Answer: A

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. Answer B 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 135
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: AD

Explanation:
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 B is incorrect. Simplify the design principle is included in the General Principle 3.

NEW QUESTION 140
Which of the following strategies is used to minimize the effects of a disruptive event on a company, and is created to prevent interruptions to normal business activity?

A. Continuity of Operations Plan
B. Contingency Plan
C. Disaster Recovery Plan
D. Business Continuity Plan

Answer: D

Explanation:
BCP is a strategy to minimize the consequence of the instability and to allow for the continuation of business processes. The goal of BCP is to minimize the effects of a disruptive event on a company, and is formed to avoid interruptions to normal business activity. 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. 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 B is incorrect. 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 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.

NEW QUESTION 144
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: ABD

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 145
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

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). Answer B is incorrect. The system owner has the responsibility of informing the key officials within the organization of the requirements for a security C&A of the information system. He makes the resources available, and provides the relevant documents to support the process. Answer A is incorrect. An Information System Security Officer (ISSO) plays the role of a supporter. The responsibilities of an Information System Security Officer (ISSO) are as follows: Manages the security of the information system that is slated for Certification & Accreditation (C&A). Insures the information systems configuration with the agency's information security policy. Supports the information system owner/information owner for the completion of security- related responsibilities. Takes part in the formal configuration management process. Prepares Certification & Accreditation (C&A) packages. Answer D is incorrect. The CISO has the responsibility of carrying out the CIO's FISMA responsibilities. He manages the information security program functions.

NEW QUESTION 149
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: ABD

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. Answer B is incorrect. Financial assessment does not come under the ISO/IEC 27002 standard.

NEW QUESTION 154
In which of the following phases of the DITSCAP process does Security Test and Evaluation (ST&E) occur?

A. Phase 2
B. Phase 4
C. Phase 3
D. Phase 1

Answer: C

Explanation:
Security Test and Evaluation (ST&E) occurs in Phase 3 of the DITSCAP C&A process. Answer D is incorrect. The Phase 1 of DITSCAP C&A is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. The Phase 1 starts with the input of the mission need. This phase comprises three process activities: Document mission need Registration Negotiation Answer A is incorrect. The Phase 2 of DITSCAP C&A is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. This phase takes place between the signing of the initial version of the SSAA and the formal accreditation of the system. This phase verifies security requirements during system development. The process activities of this phase are as follows: Configuring refinement of the SSAA System development Certification analysis Assessment of the Analysis Results Answer B is incorrect. The Phase 4 of DITSCAP C&A is known as Post Accreditation. This phase starts after the system has been accredited in the Phase 3. The goal of this phase is to continue to operate and manage the system and to ensure that it will maintain an acceptable level of residual risk. The process activities of this phase are as follows: System operations Security operations Maintenance of the SSAA Change management Compliance validation

NEW QUESTION 156
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

Explanation:
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 co-operation between NSA and U.S. military cryptanalysis agencies. NSA's work is limited to communications intelligence. It does not perform field or human intelligence activities. Answer B is incorrect. The 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 161
NIST SP 800-53A defines three types of interview depending on the level of assessment conducted. Which of the following NIST SP 800-53A interviews consists of informal and ad hoc interviews?

A. Comprehensive
B. Significant
C. Abbreviated
D. Substantial

Answer: C

Explanation:
Abbreviated interview consists of informal and ad hoc interviews. Answer D is incorrect. Substantial interview consists of informal and structured interviews. Answer A is incorrect. Comprehensive interview consists of formal and structured interviews. Answer B is incorrect. There is no such type of interview in NIST SP 800-53A.

NEW QUESTION 165
Which of the following are the principle duties performed by the BIOS during POST (power- on-self-test)? Each correct answer represents a part of the solution. Choose all that apply.

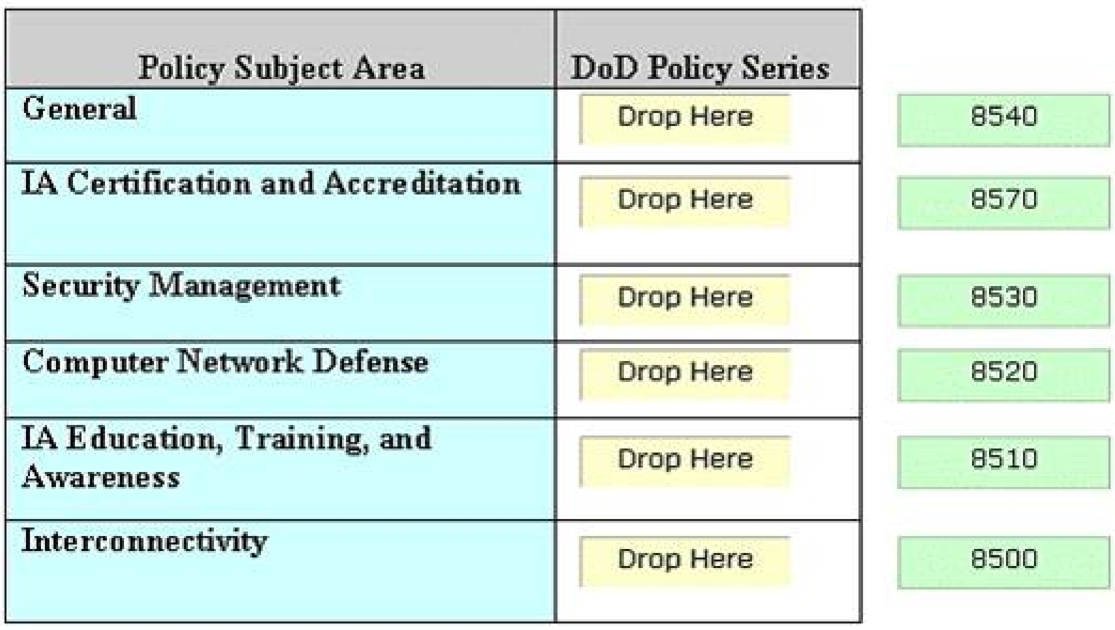
A. It provides a user interface for system's configuration.
B. It identifies, organizes, and selects boot devices.
C. It delegates control to other BIOS, if it is required.
D. It discovers size and verifies system memory.
E. It verifies the integrity of the BIOS code itself.

F. It interrupts the execution of all running programs.

Answer: ABCDE

Explanation:
The principle duties performed by the BIOS during POST (power-on-self- test) are as follows: It verifies the integrity of the BIOS code itself. It discovers size and verifies system memory. It discovers, initializes, and catalogs all system hardware. It delegates control to other BIOS if it is required. It provides a user interface for system's configuration. It identifies, organizes, and selects boot devices. It executes the bootstrap program. Answer F is incorrect. The BIOS does not interrupt the execution of all running programs.

NEW QUESTION 170
DRAG DROP
Drag and drop the correct DoD Policy Series at their appropriate places.

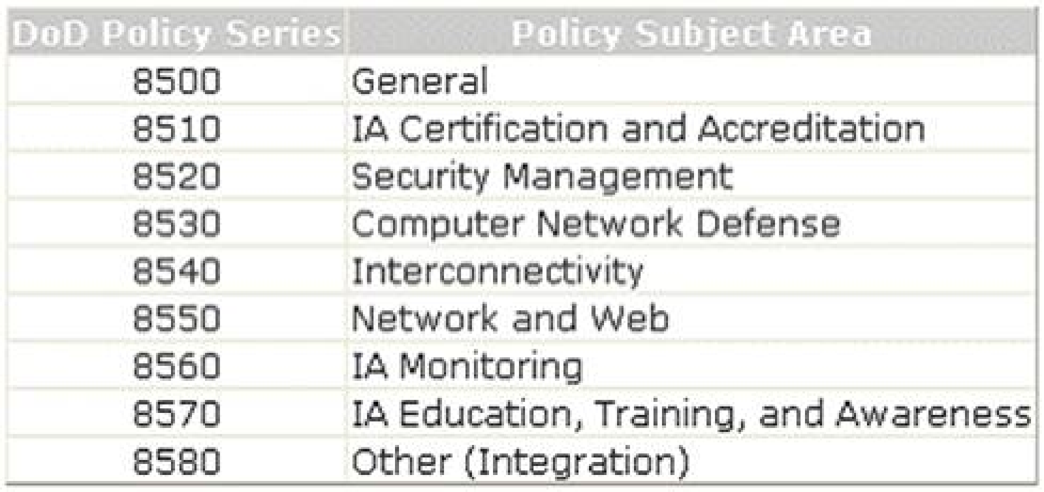


Policy Subject Area	DoD Policy Series	
General	Drop Here	8540
IA Certification and Accreditation	Drop Here	8570
Security Management	Drop Here	8530
Computer Network Defense	Drop Here	8520
IA Education, Training, and Awareness	Drop Here	8510
Interconnectivity	Drop Here	8500

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The various DoD policy series are as follows:



DoD Policy Series	Policy Subject Area
8500	General
8510	IA Certification and Accreditation
8520	Security Management
8530	Computer Network Defense
8540	Interconnectivity
8550	Network and Web
8560	IA Monitoring
8570	IA Education, Training, and Awareness
8580	Other (Integration)

NEW QUESTION 171
Which of the following are examples of passive attacks? Each correct answer represents a complete solution. Choose all that apply.

A. Dumpster diving
B. Placing a backdoor
C. Eavesdropping
D. Shoulder surfing

Answer: ACD

Explanation:
In eavesdropping, dumpster diving, and shoulder surfing, the attacker violates the confidentiality of a system without affecting its state. Hence, they are considered passive attacks.

NEW QUESTION 176
John works as a security manager for SoftTech Inc. He is working with his team on the disaster recovery management plan. One of his team members has a doubt related to the most cost effective DRP testing plan. According to you, which of the following disaster recovery testing plans is the most cost-effective and efficient way to identify areas of
overlap in the plan before conducting more demanding training exercises?

A. Full-scale exercise
B. Walk-through drill
C. Structured walk-through test

D. Evacuation drill

Answer: C

Explanation:
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 A is incorrect. In full-scale exercise, the critical systems run at an alternate site. Answer B is incorrect. The emergency management group and response teams actually perform their emergency response functions by walking through the test, without actually initiating recovery procedures. But it is not much cost effective. Answer D is incorrect. It is a test performed when personnel walks through the evacuation route to a designated area where procedures for accounting for the personnel are tested.

NEW QUESTION 181
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: ACD

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 Answer B is incorrect. Information systems acquisition, development, and maintenance is an International information security standard.

NEW QUESTION 184
"Enhancing the Development Life Cycle to Produce Secure Software" summarizes the tools and practices that are helpful in producing secure software. What are these tools and practices? Each correct answer represents a complete solution. Choose three.

A. Leverage attack patterns
B. Compiler security checking and enforcement
C. Tools to detect memory violations
D. Safe software libraries
E. Code for reuse and maintainability

Answer: BCD

Explanation:
The tools and practices that are helpful in producing secure software are summarized in the report "Enhancing the Development Life Cycle to Produce Secure Software". The tools and practices are as follows: Compiler security checking and enforcement Safe software libraries Runtime error checking and safety enforcement Tools to detect memory violations Code obfuscation Answer A and E are incorrect. These are secure coding principles and practices of defensive coding.

NEW QUESTION 186
Which of the following elements of the BCP process emphasizes on creating the scope and the additional elements required to define the parameters of the plan?

A. Business continuity plan development
B. Plan approval and implementation
C. Business impact analysis
D. Scope and plan initiation

Answer: D

Explanation:
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 A is incorrect. The business continuity plan development refers to the utilization of the information collected in the Business Impact Analysis (BIA) for the creation of the recovery strategy plan to support the critical business functions. The information gathered from the BIA is mapped out to make a strategy for creating a continuity plan. The business continuity plan development process includes the areas of plan implementation, plan testing, and ongoing plan maintenance. This phase also consists of defining and documenting the continuity strategy. Answer B is incorrect. The plan approval and implementation process involves creating enterprise-wide awareness of the plan, getting the final senior management signoff, and implementing a maintenance procedure for updating the plan as required.

NEW QUESTION 188
Which of the following intrusion detection systems (IDS) monitors network traffic and compares it against an established baseline?

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

D. Signature-based

Answer: C

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

NEW QUESTION 192
Which of the following phases of NIST SP 800-37 C&A methodology examines the residual risk for acceptability, and prepares the final security accreditation package?

A. Security Accreditation
B. Initiation
C. Continuous Monitoring
D. Security Certification

Answer: A

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 195
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

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. 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 198
You work as the Senior Project manager in Dotcoiss Inc. Your company has started a software project using configuration management and has completed 70% of it. You need to ensure that the network infrastructure devices and networking standards used in this
project are installed in accordance with the requirements of its detailed project design documentation. Which of the following procedures will you employ to accomplish the task?

A. Configuration identification
B. Configuration control
C. Functional configuration audit
D. Physical configuration audit

Answer: D

Explanation:
Physical Configuration Audit (PCA) is one of the practices used in Software Configuration Management for Software Configuration Auditing. The purpose of the software PCA is to ensure that the design and reference documentation is consistent with the as-built software product. PCA checks and matches the really implemented layout with the documented layout. Answer B is incorrect. Functional Configuration Audit or FCA is one of the practices used in Software Configuration Management for Software Configuration Auditing. FCA occurs either at delivery or at the moment of effecting the change. A Functional Configuration Audit ensures that functional and performance attributes of a configuration item are achieved. Answer B is incorrect. Configuration control is a procedure of the Configuration management. Configuration control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them. It supports the change of the functional and physical attributes of software at various points in time, and performs systematic control of changes to the identified attributes. Answer A is incorrect. Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined. Baselining an attribute forces formal configuration change control processes to be effected in the event that these attributes are changed.

NEW QUESTION 202
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: D

Explanation:
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 B 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 203
Fill in the blank with an appropriate security type. applies the internal security policies of the software applications when they are deployed.

A. Programmatic security

Answer: A

Explanation:
Programmatic security applies the internal security policies of the software applications when they are deployed. In this type of security, the code of the software application controls the security behavior, and authentication decisions are made based on the business logic, such as the user role or the task performed by the user in a specific security context.

NEW QUESTION 205
Which of the following approaches can be used to build a security program? Each correct answer represents a complete solution. Choose all that apply.

A. Right-Up Approach
B. Left-Up Approach
C. Top-Down Approach
D. Bottom-Up Approach

Answer: CD

Explanation:
Top-Down Approach is an approach to build a security program. The initiation, support, and direction come from the top management and work their way through middle management and then to staff members. It is treated as the best approach. This approach ensures that the senior management, who is ultimately responsible for protecting the company assets, is driving the program. Bottom-Up Approach is an approach to build a security program. The lower-end team comes up with a security control or a program without proper management support and direction. It is less effective and doomed to fail. Answer A and B are incorrect. No such types of approaches exist

NEW QUESTION 206
Which of the following is the most secure method of authentication?

A. Biometrics
B. Username and password
C. Anonymous
D. Smart card

Answer: A

Explanation:
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 B 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 211
Which of the following NIST Special Publication documents provides a guideline on questionnaires and checklists through which systems can be evaluated for compliance against specific control objectives?

A. NIST SP 800-37
B. NIST SP 800-26
C. NIST SP 800-53A
D. NIST SP 800-59
E. NIST SP 800-53
F. NIST SP 800-60

Answer: B

Explanation:
NIST SP 800-26 (Security Self-Assessment Guide for Information Technology Systems) provides a guideline on questionnaires and checklists through which systems can be evaluated for compliance against specific control objectives. Answer A, E, C, D, and F are incorrect. 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 216
You work as a project manager for BlueWell Inc. You are preparing to plan risk responses for your project with your team. How many risk response types are available for a negative risk event in the project?

A. Three
B. Seven
C. One
D. Four

Answer: D

Explanation:
There are four risk responses available for a negative risk event. The risk response strategies for negative risks are: Avoid: It involves altering the project management plan to remove the threats completely. Transfer: It requires shifting some or all of the negative effects of a threat including the ownership of response, to a third party. Mitigate: It implies a drop in the probability and impact of an unfavorable risk event to be within suitable threshold limits. Accept: It delineates that the project plan will not be changed to deal with the risk. Management may develop a contingency plan if the risk occurs. It is used for both negative and positive risks. Answer B is incorrect. There are four responses for negative risk events. Answer A is incorrect. There are four, not three, responses for negative risk events. Do not forget that acceptance can be used for negative risk events. Answer B is incorrect. There are seven total risk responses, four of which can be used for negative risk events.

NEW QUESTION 217
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: BCD

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. Answer A is incorrect. In order to save all the data from the SQL injection attack, you should minimize database permissions.

NEW QUESTION 218
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: ABD

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 Answer B is incorrect. Determining what level of classification the information requires is the responsibility of the owner.

NEW QUESTION 222
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

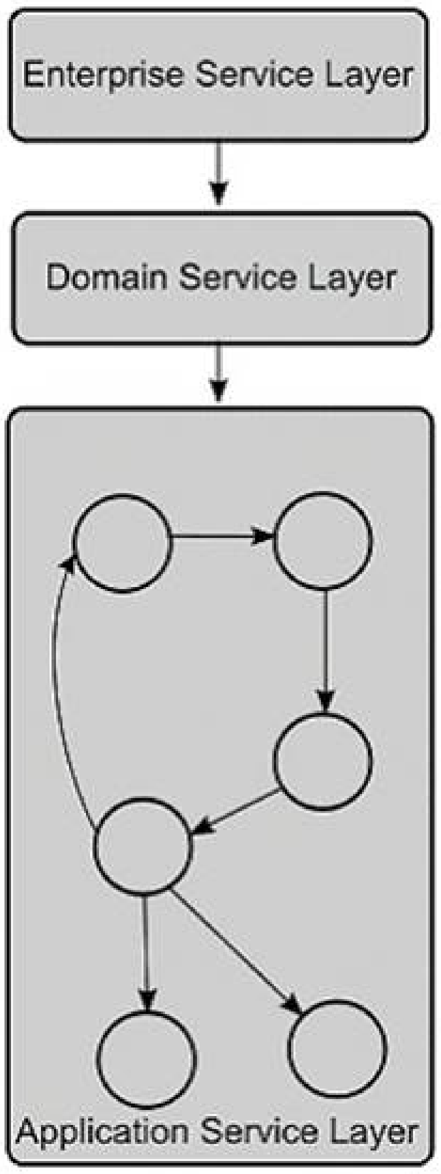
Explanation:
Microsoft Baseline Security Analyzer (MBSA) is a tool that includes a graphical and command line interface that can perform local or remote scans of Windows systems. It runs on computers running Windows 2000, Windows XP, or Windows Server 2003 operating system. MBSA scans for common security 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. Answer B, D, and A are incorrect. These are invalid options.

NEW QUESTION 225
Which of the following security architectures defines how to integrate widely disparate applications for a world that is Web-based and uses multiple implementation platforms?

A. Sherwood Applied Business Security Architecture
B. Enterprise architecture
C. Service-oriented architecture
D. Service-oriented modeling and architecture

Answer: C

Explanation:
In computing, a service-oriented architecture (SOA) is a flexible set of design
principles used during the phases of systems development and integration. A deployed SOA-based architecture will provide a loosely-integrated suite of services that can be used within multiple business domains. SOA also generally provides a way for consumers of services, such as web-based applications, to be aware of available SOA-based services. For example, several disparate departments within a company may develop and deploy SOA services in different implementation languages; their respective clients will benefit from a well understood, well defined interface to access them. XML is commonly used for interfacing with SOA services, though this is not required. SOA defines how to integrate widely disparate applications for a world that is Web-based and uses multiple implementation platforms. Rather than defining an API, SOA defines the interface in terms of protocols and functionality. An endpoint is the entry point for such an SOA implementation.



(Layer interaction in Service-oriented architecture) Answer A is incorrect. SABSA (Sherwood Applied Business Security Architecture) is a framework and methodology for Enterprise Security Architecture and Service Management. SABSA is a model and a methodology for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives. The primary characteristic of the SABSA model is that everything must be derived from an analysis of the business requirements for security, especially those in which security has an enabling function through which new business opportunities can be developed and exploited. Answer D is incorrect. The service-oriented modeling and architecture (SOMA) includes an analysis and design method that extends traditional object-oriented and component-based analysis and design methods to include concerns relevant to and supporting SOAnswer B is incorrect. Enterprise architecture describes the terminology, the composition of subsystems, and their relationships with the external environment, and the guiding principles for the design and evolution of an enterprise.

NEW QUESTION 229
Which of the following DoD policies establishes policies and assigns responsibilities to achieve DoD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network-centric warfare?

A. DoDI 5200.40
B. DoD 8500.1 Information Assurance (IA)
C. DoD 8510.1-M DITSCAP
D. DoD 8500.2 Information Assurance Implementation

Answer: B

Explanation:
DoD 8500.1 Information Assurance (IA) sets up policies and allots responsibilities to achieve DoD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network-centric warfare. DoD 8500.1 also summarizes the roles and responsibilities for the persons responsible for carrying out the IA policies. Answer D is incorrect. The DoD 8500.2 Information Assurance Implementation pursues 8500.1. It provides assistance on how to implement policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks. DoD Instruction 8500.2 allots tasks and sets procedures for applying integrated layered protection of the DOD information systems and networks in accordance with the DoD 8500.1 policy. It also provides some important guidelines on how to implement an IA program. Answer A is incorrect. DoDI 5200.40 executes the policy, assigns responsibilities, and recommends procedures under reference for Certification and Accreditation(C&A) of

information technology (IT). Answer B is incorrect. DoD 8510.1-M DITSCAP provides standardized activities leading to accreditation, and establishes a process and management baseline.

NEW QUESTION 234
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

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. 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 B is incorrect. Change Management is used to ensure that standardized methods and procedures are used for efficient handling of all changes.

NEW QUESTION 236
What are the differences between managed and unmanaged code technologies? Each correct answer represents a complete solution. Choose two.

A. Managed code is referred to as Hex code, whereas unmanaged code is referred to as byte code.
B. C and C++ are the examples of managed code, whereas Java EE and Microsoft.NET are the examples of unmanaged code.
C. Managed code executes under management of a runtime environment, whereas unmanaged code is executed by the CPU of a computer system.
D. Managed code is compiled into an intermediate code format, whereas unmanaged code is compiled into machine code.

Answer: CD

Explanation:
Programming languages are categorized into two technologies: 1.Managed code: This computer program code is compiled into an intermediate code format. Managed code is referred to as byte code. It executes under the management of a runtime environment. Java EE and Microsoft.NET are the examples of managed code. 2.Unmanaged code: This computer code is compiled into machine code. Unmanaged code is executed by the CPU of a computer system. C and C++ are the examples of unmanaged code. Answer A is incorrect. Managed code is referred to as byte code. Answer B is incorrect. C and C++ are the examples of unmanaged code, whereas Java EE and Microsoft.NET are the examples of managed code.

NEW QUESTION 239
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: ABCDE

Explanation:
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 244
In which type of access control do user ID and password system come under?

A. Physical
B. Technical
C. Power
D. Administrative

Answer: B

Explanation:
Technical access controls include IDS systems, encryption, network segmentation, and antivirus controls. Answer D is incorrect. The policies and procedures implemented by an organization come under administrative access controls. Answer A is incorrect. Security guards, locks on the gates, and alarms come under physical access controls. Answer B is incorrect. There is no such type of access control as power control.

NEW QUESTION 249

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

Explanation:
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 B 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 254
......