ISC2

Exam Questions CSSLP

Certified Information Systems Security Professional

NEW QUESTION 1
Which of the following NIST Special Publication documents provides a guideline on network security testing?

A. NIST SP 800-42
B. NIST SP 800-53A
C. NIST SP 800-60
D. NIST SP 800-53
E. NIST SP 800-37
F. NIST SP 800-59

Answer: A

Explanation:
NIST SP 800-42 provides a guideline on network security testing. Answer E, D, B, F, and C 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 2
A Web-based credit card company had collected financial and personal details of Mark before issuing him a credit card. The company has now provided Mark's financial and personal details to another company. Which of the following Internet laws has the credit card issuing company violated?

A. Trademark law
B. Security law
C. Privacy law
D. Copyright law

Answer: C

Explanation:
The credit card issuing company has violated the Privacy law. According to the Internet Privacy law, a company cannot provide their customer's financial and personal details to other companies. Answer A is incorrect. Trademark laws facilitate the protection of trademarks around the world. Answer B is incorrect. There is no law such as Security law. Answer D is incorrect. The Copyright law protects original works or creations of authorship including literary, dramatic, musical, artistic, and certain other intellectual works.

NEW QUESTION 3
The DoD 8500 policy series represents the Department's information assurance strategy. Which of the following objectives are defined by the DoD 8500 series? Each correct answer represents a complete solution. Choose all that apply.

A. Defending systems
B. Providing IA Certification and Accreditation
C. Providing command and control and situational awareness
D. Protecting information

Answer: ACD

Explanation:
The various objectives of the DoD 8500 series are as follows: Protecting information Defending systems Providing command and control and situational awareness Making sure that the information assurance is integrated into processes Increasing security awareness throughout the DoD's workforce

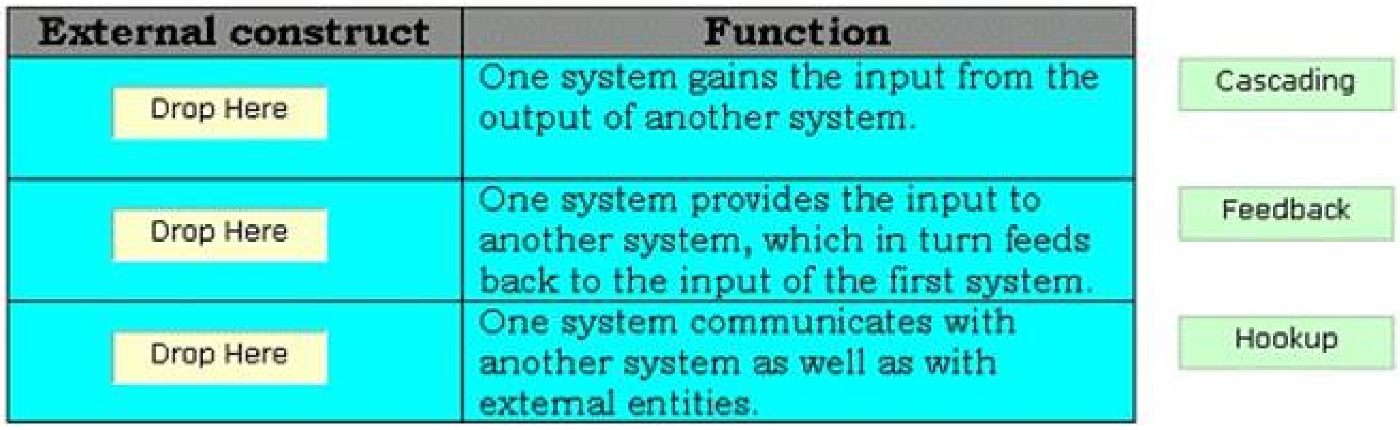
NEW QUESTION 4
Which of the following technologies is used by hardware manufacturers, publishers, copyright holders and individuals to impose limitations on the usage of digital content and devices?

A. Hypervisor
B. Grid computing
C. Code signing
D. Digital rights management

Answer: D

Explanation:
Digital rights management (DRM) is an access control technology used by hardware manufacturers, publishers, copyright holders and individuals to impose limitations on the usage of digital content and devices. It describes the technology that prevents the uses of digital content that were not desired or foreseen by the content provider. DRM does not refer to other forms of copy protection which can be circumvented without modifying the file or device, such as serial numbers or keyfiles. It can also refer to restrictions associated with specific instances of digital works or devices. Answer C is incorrect. Code signing is the process of digitally signing executables and scripts in order to confirm the software author, and guarantee that the code has not been altered or corrupted since it is signed by use of a cryptographic hash. Answer A is incorrect. A hypervisor is a virtualization technique that allows multiple operating systems (guests) to run concurrently on a host computer. It is also called the virtual machine monitor (VMM). The hypervisor provides a virtual operating platform to the guest operating systems and checks their execution process. It provides isolation to the host's resources. The hypervisor is installed on server hardware. Answer B is incorrect. Grid computing refers to the combination of computer resources from multiple administrative domains to achieve a common goal.

NEW QUESTION 5
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.

Solution:
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.

Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 6
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 7
Which of the following scanning techniques helps to ensure that the standard software configuration is currently with the latest security patches and software, and helps to locate uncontrolled or unauthorized software?

A. Port Scanning
B. Discovery Scanning
C. Server Scanning
D. Workstation Scanning

Answer: D

Explanation:
Workstation scanning provides help to ensure that the standard software configuration exists with the most recent security patches and software. It helps to locate uncontrolled or unauthorized software. A full workstation vulnerability scan of the standard corporate desktop configuration must be implemented on a regularly basis. Answer B is incorrect. The discovery scanning technique is used to gather adequate information regarding each network device to identify what type of device it is, its operating system, and if it is running any externally vulnerable services, like Web services, FTP, or email.
Answer C is incorrect. A full server vulnerability scan helps to determine if the server OS has been configured to the corporate standards and identify if applications have been updated with the latest security patches and software versions. Answer A is incorrect. Port scanning technique describes the process of sending a data packet to a port to gather information about the state of the port.

NEW QUESTION 8
What are the security advantages of virtualization, as described in the NIST Information Security and Privacy Advisory Board (ISPAB) paper "Perspectives on Cloud Computing and Standards"? Each correct answer represents a complete solution. Choose three.

A. It increases capabilities for fault tolerant computing.

B. It adds a layer of security for defense-in-depth.
C. It decreases exposure of weak software.
D. It decreases configuration effort.

Answer: ABC

Explanation:
The security advantages of virtualization are as follows: It adds a layer of security for defense-in-depth. It provides strong encapsulation of errors. It increases intrusion detection through introspection. It decreases exposure of weak software. It increases the flexibility for discovery. It increases capabilities for fault tolerant computing using rollback and snapshot features. Answer D is incorrect. Virtualization increases configuration effort because of complexity of the virtualization layer and composite system.

NEW QUESTION 9
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 10
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 11
Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in. What are the different categories of penetration testing? Each correct answer represents a complete solution. Choose all that apply.

A. Open-box
B. Closed-box
C. Zero-knowledge test
D. Full-box
E. Full-knowledge test
F. Partial-knowledge test

Answer: ABCEF

Explanation:
The different categories of penetration testing are as follows: Open-box: In this category of penetration testing, testers have access to internal system code. This mode is basically suited for Unix or Linux. Closed-box: In this category of penetration testing, testers do not have access to closed systems. This method is good for closed systems. Zero-knowledge test: In this category of penetration testing, testers have to acquire information from scratch and they are not supplied with information concerning the IT system. Partial-knowledge test: In this category of penetration testing, testers have knowledge that may be applicable to a specific type of attack and associated vulnerabilities. Full-knowledge test: In this category of penetration testing, testers have massive knowledge concerning the information system to be evaluated. Answer D is incorrect. There is no such category of penetration testing.

NEW QUESTION 12
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 13
Which of the following acts is used to recognize the importance of information security to the economic and national security interests of the United States?

A. Computer Misuse Act
B. Lanham Act
C. Computer Fraud and Abuse Act
D. FISMA

Answer: D

Explanation:
The Federal Information Security Management Act of 2002 is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002. The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA has brought attention within the federal government to cybersecurity and explicitly emphasized a 'risk-based policy for cost-effective security'. FISMA requires agency program officials, chief information officers, and Inspectors Generals (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget (OMB). OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act. Answer B is incorrect. The Lanham Act is a piece of legislation that contains the federal statutes of trademark law
in the United States. The Act prohibits a number of activities, including trademark infringement, trademark dilution, and false advertising. It is also called Lanham Trademark Act. Answer A is incorrect. The Computer Misuse Act 1990 is an act of the UK Parliament which states the following statement: Unauthorized access to the computer material is punishable by 6 months imprisonment or a fine "not exceeding level 5 on the standard scale" (currently 5000). Unauthorized access with the intent to commit or facilitate commission of further offences is punishable by 6 months/maximum fine on summary conviction or 5 years/fine on indictment. Unauthorized modification of computer material is subject to the same sentences as section 2 offences. Answer B is incorrect. The Computer Fraud and Abuse Act is a law passed by the United States Congress in 1984 intended to reduce cracking of computer systems and to address federal computer-related offenses. The Computer Fraud and Abuse Act (codified as 18
U.S.C. 1030) governs cases with a compelling federal interest, where computers of the federal government or certain financial institutions are involved, where the crime itself is interstate in nature, or computers used in interstate and foreign commerce. It was amended in 1986, 1994, 1996, in 2001 by the USA PATRIOT Act, and in 2008 by the Identity Theft Enforcement and Restitution Act. Section (b) of the act punishes anyone who not just commits or attempts to commit an offense under the Computer Fraud and Abuse Act but also those who conspire to do so.

NEW QUESTION 14
Which of the following phases of DITSCAP includes the activities that are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle?

A. Phase 2, Verification
B. Phase 3, Validation
C. Phase 1, Definition
D. Phase 4, Post Accreditation Phase

Answer: D

Explanation:
Phase 4, Post Accreditation Phase, of the DITSCAP includes the activities that are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle. Answer B is incorrect. Phase 1, Definition, focuses on understanding the mission, the environment, and the architecture in order to determine the security requirements and level of effort necessary to achieve accreditation. Answer A is incorrect. Phase 2, Verification, verifies the evolving or modified system's compliance with the information agreed on in the System Security Authorization Agreement (SSAA). Answer B is incorrect. Phase 3 validates the compliance of a fully integrated system with the information stated in the SSAA.

NEW QUESTION 15
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 16
FIPS 199 defines the three levels of potential impact on organizations: low, moderate, and high. Which of the following are the effects of loss of confidentiality,

integrity, or availability in a high level potential impact?

A. The loss of confidentiality, integrity, or availability might result in a major damage to organizational assets.
B. The loss of confidentiality, integrity, or availability might result in severe damages like life threatening injuries or loss of life.
C. The loss of confidentiality, integrity, or availability might result in major financial losses.
D. The loss of confidentiality, integrity, or availability might cause severe degradation in or loss of mission capability to an extent.

Answer: ABCD

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

NEW QUESTION 17
Elizabeth is a project manager for her organization and she finds risk management to be very difficult for her to manage. She asks you, a lead project manager, at what stage in the project will risk management become easier. What answer best resolves the difficulty of risk management practices and the effort required?

A. Risk management only becomes easier when the project moves into project execution.
B. Risk management only becomes easier when the project is closed.
C. Risk management is an iterative process and never becomes easier.
D. Risk management only becomes easier the more often it is practiced.

Answer: D

Explanation:
According to the PMBOK, "Like many things in project management, the more it is done the easier the practice becomes." Answer B is incorrect. This answer is not the best choice for the project. Answer A is incorrect. Risk management likely becomes more difficult in project execution that in other stages of the project. Answer B is incorrect. Risk management does become easier the more often it is done.

NEW QUESTION 18
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. What are the different types of NIACAP accreditation? Each correct answer represents a complete solution. Choose all that apply.

A. Site accreditation
B. Type accreditation
C. Secure accreditation
D. System accreditation

Answer: ABD

Explanation:
NIACAP accreditation is of three types depending on what is being certified. They are as follows: 1.Site accreditation: This type of accreditation evaluates the applications and systems at a specific, self contained location. 2.Type accreditation: This type of accreditation evaluates an application or system that is distributed to a number of different locations. 3.System accreditation: This accreditation evaluates a major application or general support system. Answer B is incorrect. No such type of NIACAP accreditation exists.

NEW QUESTION 19
Which of the following processes will you involve to perform the active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures?

A. Penetration testing
B. Baselining
C. Risk analysis
D. Compliance checking

Answer: A

Explanation:
A penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered. It is a component of a full security audit. Answer B is incorrect. Risk analysis is the science of risks and their probability and evaluation in a business or a process. It is an important factor in security enhancement and prevention in a system. Risk analysis should be performed as part of the risk management process for each project. The outcome of the risk analysis would be the creation or review of the risk register to identify and quantify risk elements to the project and their potential impact. Answer D is incorrect. Compliance checking performs the reviews for safeguards and controls to verify whether the entity is complying with particular procedures, rules or not. It includes the inspection of operational systems to guarantee that hardware and software controls have been correctly implemented and maintained. Compliance checking covers the activities such as penetration testing and vulnerability assessments. Compliance checking must be performed by skilled persons, or by an automated software package. Answer B is incorrect. Baselining is a method for analyzing the performance of computer networks. The method is marked by comparing the current performance to a historical metric, or "baseline". For example, if a user measured the performance of a network switch over a period of time, he could use that performance figure as a comparative baseline if he made a configuration change to the switch.

NEW QUESTION 20
You work as an analyst for Tech Perfect Inc. You want to prevent information flow that may cause a conflict of interest in your organization representing competing clients. Which of the following security models will you use?

A. Bell-LaPadula model
B. Chinese Wall model
C. Clark-Wilson model
D. Biba model

Answer: B

Explanation:
The Chinese Wall Model is the basic security model developed by Brewer and Nash. This model prevents information flow that may cause a conflict of interest in an organization representing competing clients. The Chinese Wall Model provides both privacy and integrity for datAnswer D is incorrect. The Biba model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject. Answer B 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 A 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.

NEW QUESTION 21
......