CSSLP[Q&As]

Certified Secure Software Lifecycle Professional Practice Test

Pass ISC CSSLP Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/csslp.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by ISC Official Exam Center

QUESTION 1

Which of the following classification levels defines the information that, if disclosed to the unauthorized parties, could be reasonably expected to cause exceptionally grave damage to the national security?

A. Secret information

B. Unclassified information

C. Confidential information

D. Top Secret information

Correct Answer: D

Top Secret information is the highest level of classification of material on a national level. Such material would cause "exceptionally grave damage" to national security if publicly available. Answer: A is incorrect. Secret information is that, if disclosed to unauthorized parties, could be expected to cause serious damage to the national security, but it is not the best answer for the above question. Answer: C is incorrect. Such material would cause "damage" or be "prejudicial" to national security if publicly available. Answer: B is incorrect. Unclassified information, technically, is not a classification level, but is used for government documents that do not have a classification listed above. Such documents can sometimes be viewed by those without security clearance.

QUESTION 2

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

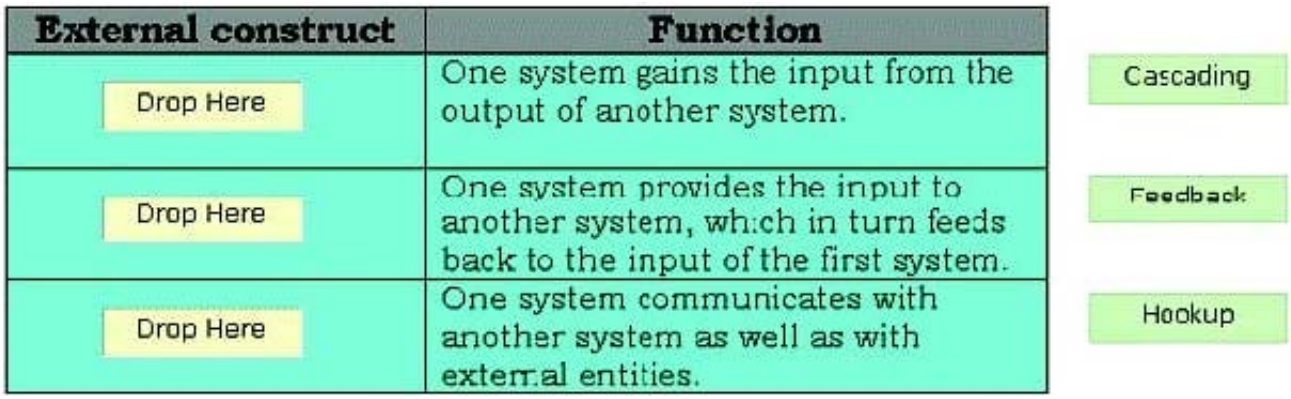
D. IDMS

Correct Answer: C

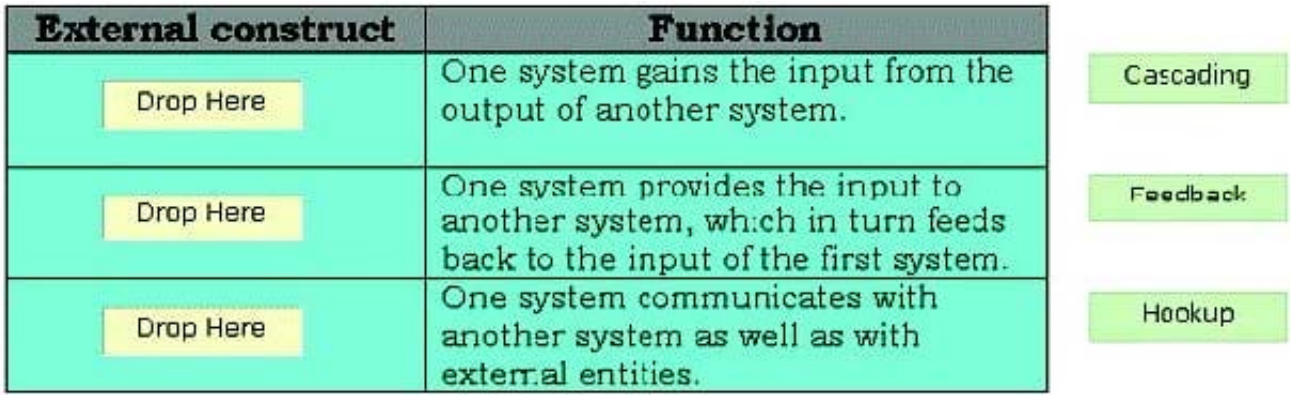
Microsoft Baseline Security Analyzer (MBSA) is a tool that includes a graphical and command line interface that can perform local or remote scans of Windows systems. It runs on computers running Windows 2000, Windows XP, or Windows Server 2003 operating system. MBSA scans for common security misconfigurations 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.

QUESTION 3

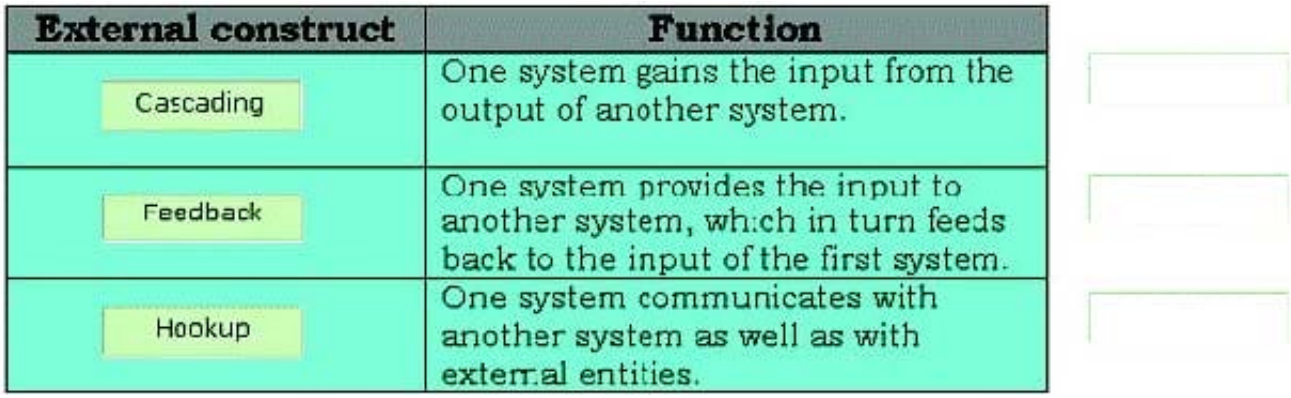
Drag and drop the appropriate external constructs in front of their respective functions.



Select and Place:



Correct Answer:



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.

QUESTION 4

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

Correct Answer: ABD

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:

C is incorrect. No such type of NIACAP accreditation exists.

QUESTION 5

System Authorization is the risk management process. System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. What are the different phases of System Authorization Plan? Each

correct answer represents a part of the solution.

Choose all that apply.

A. Post-certification

B. Post-Authorization

C. Authorization

D. Pre-certification

E. Certification

Correct Answer: BCDE

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

QUESTION 6

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

Correct Answer: C

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.

QUESTION 7

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.

Correct Answer: CD

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.

QUESTION 8

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

Correct Answer: D

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.

QUESTION 9

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

Correct Answer: B

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 and Accreditation (CandA). 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.

QUESTION 10

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

Correct Answer: A

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

QUESTION 11

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

A. Phase 3, Validation

B. Phase 1, Definition

C. Phase 2, Verification

D. Phase 4, Post Accreditation Phase

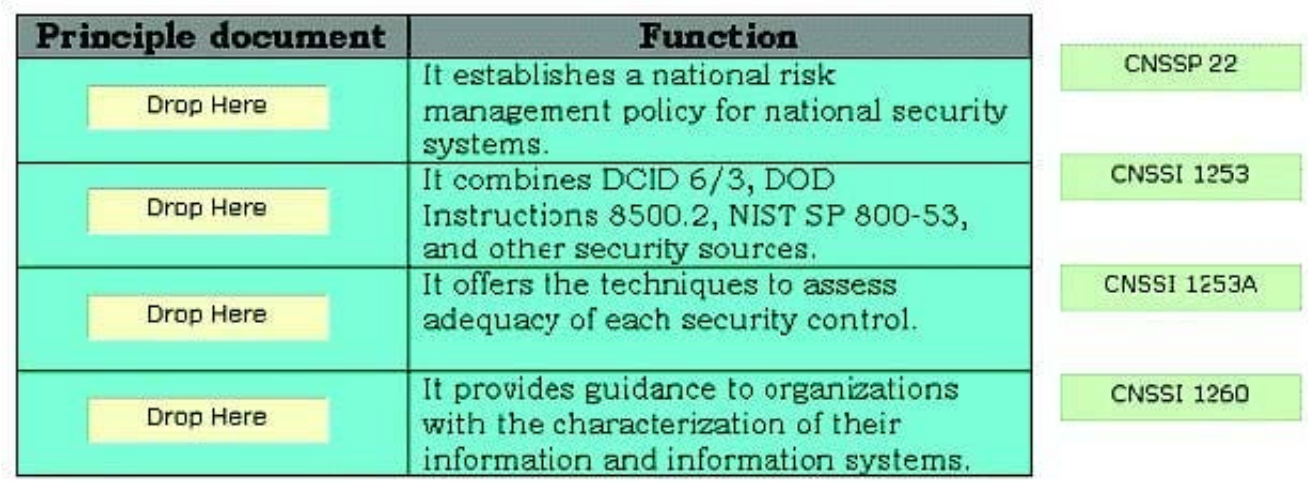
Correct Answer: D

Phase 4, Post Accreditation Phase of the DITSCAP includes the activities, which are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle. Answer: B is incorrect. Phase 1, Definition, focuses on understanding the mission, the environment, and the architecture in order to determine the security requirements and level of effort necessary to

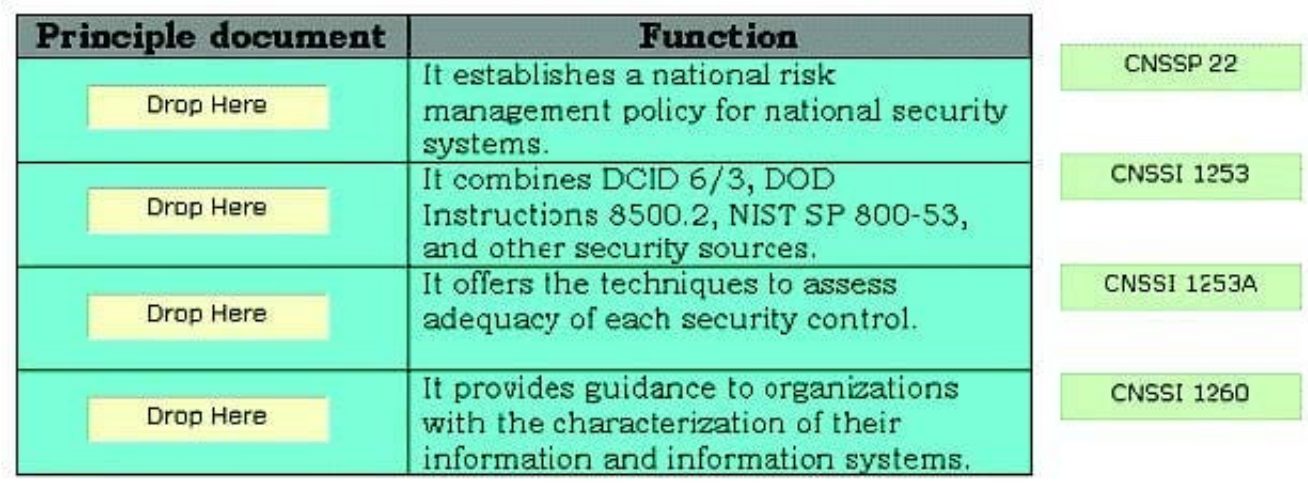
achieve accreditation. Answer: C is incorrect. Phase 2, Verification, verifies the evolving or modified system\\'s compliance with the information agreed on in the System Security Authorization Agreement (SSAA). Answer: A is incorrect. Phase 3 validates the compliance of a fully integrated system with the information stated in the SSAA.

QUESTION 12

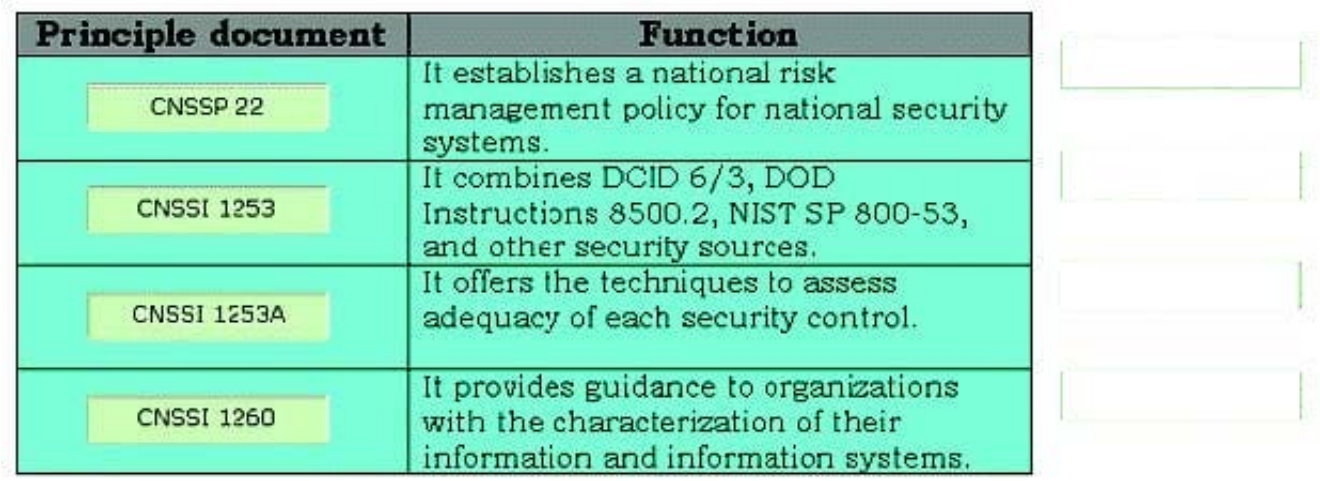
Drag and drop the appropriate principle documents in front of their respective functions.



Select and Place:



Correct Answer:



The various principle documents of transformation are as follows: CNSSP 22: It establishes a national risk management policy for national security systems. CNSSI 1199: It creates the technique in which the national security community classifies the information and information systems with regard to confidentiality, integrity, and availability. CNSSI 1253: It combines DCID 6/3, DOD Instructions 8500.2, NIST SP 800-53, and other security sources into a single cohesive repository of security controls. CNSSI 1253 A. It offers the techniques to assess adequacy of each security control. CNSSI 1260: It provides guidance to organizations with the characterization of their information and information systems. NIST 800-37, Revision 1: It defines the certification and accreditation (C and A) process. The NIST 800-37, Revision 1 is a combination of DNI, DoD, and NIST.

QUESTION 13

Which of the following models manages the software development process if the developers are limited to go back only one stage to rework?

A. Waterfall model

B. Spiral model

C. RAD model

D. Prototyping model

Correct Answer: A

In the waterfall model, software development can be managed if the developers are limited to go back only one stage to rework. If this limitation is not imposed mainly on a large project with several team members, then any developer can be working on any phase at any time, and the required rework might be accomplished several times. Answer: B is incorrect. The spiral model is a software development process combining elements of both design and prototyping-in-stages, in an effort to combine advantages of top-down and bottom-up concepts. The basic principles of the spiral model are as follows: The focus is on risk assessment and minimizing project risks by breaking a project into smaller segments and providing more ease-of- change during the development process, as well as providing the opportunity to evaluate risks and weigh consideration of project continuation throughout the life cycle. Each cycle involves a progression through the same sequence of steps, for each portion of the product and for each of its levels of elaboration, from an overall concept-of-operation document down to the coding of each individual program. Each trip around the spiral traverses the following four basic quadrants: Determine objectives, alternatives, and constraints of the iteration. Evaluate alternatives, and identify and resolve risks. Develop and verify deliverables from the iteration. Plan the next iteration. Begin each cycle with an identification of stakeholders and their win conditions, and end each cycle with review and commitment. Answer: D is incorrect. The Prototyping model is a systems development method (SDM). In this model, a prototype is created, tested, and then reworked as necessary until an adequate prototype is finally

achieved from which the complete system or product can now be developed. Answer: C is incorrect. Rapid Application Development (RAD) refers to a type of software development methodology that uses minimal planning in favor of rapid prototyping.

QUESTION 14

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

Correct Answer: D

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.

QUESTION 15

What are the subordinate tasks of the Implement and Validate Assigned IA Control phase in the DIACAP process? Each correct answer represents a complete solution. Choose all that apply.

A. Conduct validation activities.

B. Execute and update IA implementation plan.

C. Combine validation results in DIACAP scorecard.

D. Conduct activities related to the disposition of the system data and objects.

Correct Answer: ABC

The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk. The subordinate tasks of the Implement and Validate Assigned IA Control phase in the DIACAP process are as follows: Execute and update IA implementation plan. Conduct validation activities. Combine validation results in the DIACAP scorecard. Answer: D is incorrect. The activities related to the disposition of the system data and objects are conducted in the fifth phase of the DIACAP process. The fifth phase of the DIACAP process is known as Decommission System.