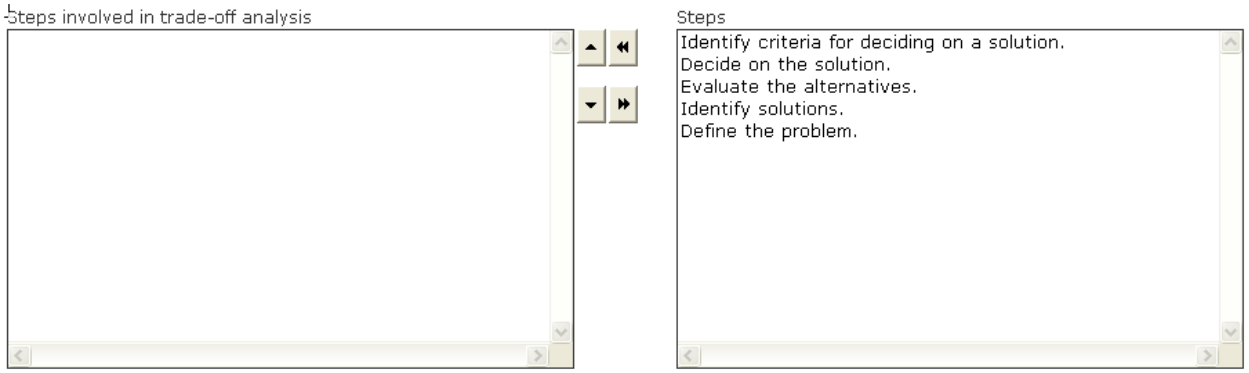
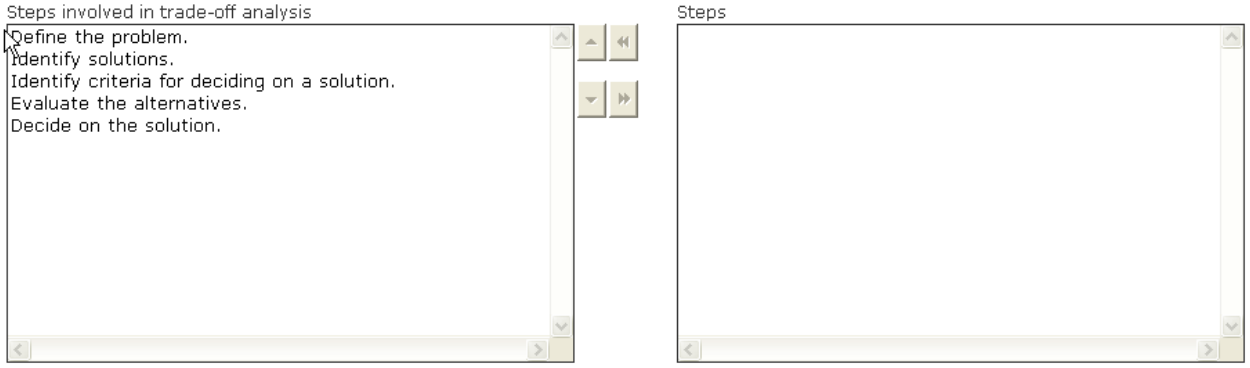
Question: 1

Choose and reorder the steps involved in the trade-off analysis.



Answer:



Explanation: The steps involved in the trade-off analysis are as follows:
1.Define the problem
2.Identify solutions
3.Identify criteria for deciding on a solution
4.Evaluate the alternatives
5.Decide on the solution

Question: 2

TQM recognizes that quality of all the processes within an organization contribute to the quality of the product. Which of the following are the most important activities in the Total Quality Management?
Each correct answer represents a complete solution. Choose all that apply.
A: Quality renewal
B: Quality improvements
C: Quality costs
D: Maintenance of quality

Answer: ABD

Explanation:

The most important activities in the Total Quality Management are as follows:
Maintenance of quality
Quality improvements
Quality renewal
Answer option C is incorrect. The concept of quality costs is a means to quantify the total cost of quality-related efforts and deficiencies.

Question: 3

Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. Which of the following statements are true about Certification and Accreditation? Each correct answer represents a complete solution. Choose two.
A: Accreditation is a comprehensive assessment of the management, operational, and technical security controls in an information system.
B: Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system.
C: Certification is the official management decision given by a senior agency official to authorize operation of an information system.
D: Accreditation is the official management decision given by a senior agency official to authorize operation of an information system.

Answer: BD

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.

Question: 4

Drag and drop the correct DoD Policy Series at their appropriate places.

Policy Subject Area	DoD Policy Series
General	Drop Here
IA Certification and Accreditation	Drop Here
Security Management	Drop Here
Computer Network Defense	Drop Here
IA Education, Training, and Awareness	Drop Here
Interconnectivity	Drop Here

8540
8570
8530
8520
8510
8500

Answer:

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

8540
8570
8530
8520
8510
8500

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)

Question: 5

You work as a system engineer for BlueWell Inc. You want to verify that the build meets its data requirements, and correctly generates each expected display and report. Which of the following tests will help you to perform the above task?
A: Functional test
B: Reliability test
C: Regression test
D: Performance test

Answer: A

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

Question: 6

Which of the following security controls will you use for the deployment phase of the SDLC to build secure software? Each correct answer represents a complete solution. Choose all that apply.
A: Vulnerability Assessment and Penetration Testing
B: Security Certification and Accreditation (C&A)
C: Risk Adjustments
D: Change and Configuration Control

Answer: ABC

Explanation:
The various security controls in the SDLC deployment phase are as follows:
Secure Installation: While performing any software installation, it should kept in mind that the security configuration of the environment should never be reduced. If it is reduced then security issues and overall risks can affect the environment. Vulnerability Assessment and Penetration Testing: Vulnerability assessments (VA) and penetration testing (PT) is used to determine the risk and attest to the strength of the software after it has been deployed. Security Certification and Accreditation (C&A): Security certification is the process used to ensure controls which are effectively implemented through established verification techniques and procedures, giving organization officials confidence that the appropriate safeguards and countermeasures are in place as means of protection. Accreditation is the

provisioning of the necessary security authorization by a senior organization official to process, store, or transmit information.Risk Adjustments: Contingency plans and exceptions should be generated so that the residual risk be above the acceptable threshold.

Question: 7

Which of the following CNSS policies describes the national policy on use of cryptomaterial by activities operating in high risk environments?
A: NSTISSP No. 6
B: CNSSP No. 14
C: NCSC No. 5
D: NSTISSP No. 7

Answer: C

Explanation:
The various CNSS policies are as follows:
NSTISSP No. 6: It describes the national policy on certification and accreditation of national security telecommunications and information systems.
NSTISSP No. 7: It describes the national policy on secure electronic messaging service.
NSTISSP No. 11: It describes the national policy governing the acquisition of information assurance (IA) and IA-enabled Information Technology (IT) products.
NSTISSP No. 101: It describes the national policy on securing voice communications.
NSTISSP No. 200: It describes the national policy on controlled access protection.
CNSSP No. 14: It describes the national policy governing the release of information assurance products and services to authorized U.S. persons or activities that are not a part of the federal government.
NCSC No. 5: It describes the national policy on use of cryptomaterial by activities operating in high risk environments.

Question: 8

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

Answer: D

Explanation:
The various MAC levels are as follows:
MAC I: It states that the systems have high availability and high integrity.

MAC II: It states that the systems have high integrity and medium availability.
MAC III: It states that the systems have basic integrity and availability.

Question: 9

Which of the following acts promote a risk-based policy for cost effective security?
Each correct answer represents a part of the solution. Choose all that apply.
A: Paperwork Reduction Act (PRA)
B: Lanham Act
C: Clinger-Cohen Act
D: Computer Misuse Act

Answer: AC

Explanation:
The Paperwork Reduction Act (PRA) and the Clinger-Cohen Act promote a risk-based policy for cost effective security.
Answer option 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 option D is incorrect. The Computer Misuse Act 1990 is an Act of the UK Parliament, which states the following statements:
Unauthorised 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. Unauthorised modification of computer material is subject to the same sentences as section 2 offences.

Question: 10

Which of the following types of CNSS issuances establishes or describes policy and programs, provides authority, or assigns responsibilities?
A: Policies
B: Directives
C: Advisory memoranda
D: Instructions

Answer: B

Explanation:
The various CNSS issuances are as follows:
Policies: It assigns responsibilities and establishes criteria (NSTISSP) or (CNSSP).
Directives: It establishes or describes policy and programs, provides authority, or assigns responsibilities

(NSTISSD). Instructions: It describes how to implement the policy or prescribes the manner of a policy (NSTISSI). Advisory memoranda: It provides guidance on policy and may cover a variety of topics involving information assurance, telecommunications security, and network security (NSTISSAM).

Question: 11

You work as a security engineer for BlueWell Inc. You want to use some techniques and procedures to verify the effectiveness of security controls in Federal Information System. Which of the following NIST documents will guide you?
A: NIST Special Publication 800-53A
B: NIST Special Publication 800-53
C: NIST Special Publication 800-37
D: NIST Special Publication 800-59

Answer: A

Explanation:
NIST has developed a suite of documents for conducting Certification & Accreditation (C&A). These documents are as follows:
1.NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information
Systems.
2.NIST Special Publication 800-53: This document provides a guideline for security controls for Federal Information Systems.
3.NIST Special Publication 800-53A: This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System.
4.NIST Special Publication 800-59: This document provides a guideline for identifying an information system as a National Security System.
5.NIST Special Publication 800-60: This document is a guide for mapping types of information and information systems to security objectives and risk levels.

Question: 12

Which of the following NIST Special Publication documents provides a guideline on network security testing?
A: NIST SP 800-53A
B: NIST SP 800-59
C: NIST SP 800-42
D: NIST SP 800-60
E: NIST SP 800-53
F:NIST SP 800-37

Answer: C

Explanation:
NIST SP 800-42 provides a guideline on network security testing.
Answer options F, E, A, B, and D 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.

Question: 13

In which of the following phases of the DITSCAP process does Security Test and Evaluation (ST&E) occur?
A: Phase 1
B: Phase 3
C: Phase 4
D: Phase 2

Answer: B

Explanation:
Security Test and Evaluation (ST&E) occurs in Phase 3 of the DITSCAP C&A process.
Answer option A 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 option D 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 option C 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