DUMPSBOSS.

# ISSEP Information Systems Security Engineering Professional

## ISC2 ISSEP

## Version Demo

**Total Demo Questions: 26**

**Total Premium Questions: 266**

**Buy Premium PDF**

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, Security Engineering Principles | 38 |
| Topic 2, Risk Management | 43 |
| Topic 3, Security Planning, Design, and Implementation | 102 |
| Topic 4, Secure Operations, Maintenance, and Disposal | 18 |
| Topic 5, Technical Management | 62 |
| Topic 6, Mix Questions | 3 |
| Total | 266 |

QUESTION NO: 1

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.** Providing IA Certification and Accreditation

**B.** Providing command and control and situational awareness

**C.** Defending systems

**D.** Protecting information

**ANSWER: A B C D**

**Explanation:**

The DoD 8500 information assurance policy framework defined a coordinated strategy for protecting Department of Defense information and the systems that create, process, store, transmit, and use it. Its strategy included **Providing IA Certification and Accreditation**, ensuring that systems received a formal security assessment and an authorization decision appropriate to their mission and risk. It also included **Providing command and control and situational awareness**, which enables leaders and security personnel to understand the security condition of DoD environments and direct defensive action. **Defending systems** is an essential objective because information assurance requires active measures to resist, detect, respond to, and recover from threats. Finally, **Protecting information** addresses safeguarding information's confidentiality, integrity, availability, authentication, and nonrepudiation as applicable. Together, these objectives connect governance and authorization activities with operational awareness, system defense, and information protection. The modern DoD cybersecurity policy successor retains the risk-management and protection focus while replacing the legacy certification-and-accreditation approach with the Risk Management Framework. See the official DoD Instruction 8500.01, Cybersecurity and NIST's Risk Management Framework resources.

**QUESTION NO: 2**

Which of the following assessment methodologies defines a six-step technical security evaluation

**A.** FITSAF

**B.** OCTAVE

**C.** FIPS 102

**D.** DITSCAP

**ANSWER: C**

**Explanation:**

FIPS 102 is correct because it specifies a six-step technical evaluation approach for assessing computer-system security. The standard, titled *Guideline for Computer Security Certification and Accreditation*, was published by the U.S. National Bureau of Standards (now NIST) to provide a structured process for determining whether a system's implemented security safeguards satisfy stated security requirements. Its technical evaluation process addresses the evidence and activities needed to examine security controls systematically, supporting the broader certification and accreditation decision process.

This is an important distinction in security engineering: certification evaluates and documents the technical security posture of a system, while accreditation is the management authorization to operate based on the resulting risk information. FIPS 102 therefore provides a historically significant, formalized methodology for conducting the technical evaluation component of system security certification. Although the publication has been withdrawn and superseded by later NIST risk-management and assessment guidance, it is the source associated with the six-step technical security evaluation described in the question. The publication record and document are available from NIST's FIPS 102 publication page. NIST's current assessment framework can also be reviewed in NIST SP 800-53A.

## QUESTION NO: 3

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.** Risk Adjustments

**B.** Security Certification and Accreditation (C&A)

**C.** Vulnerability Assessment and Penetration Testing

**D.** Change and Configuration Control

## ANSWER: A B C

**Explanation:**

Deployment is the point at which the completed system is prepared for release into its production environment and is evaluated to determine whether its security requirements have been satisfied. **Security Certification and Accreditation (C&A)** is appropriate because it provides the formal assessment and management authorization decision before the system is placed into operation. In current NIST terminology, this is implemented through the Risk Management Framework authorization process, but the underlying purpose remains validation of security controls and acceptance of residual risk.

**Vulnerability Assessment and Penetration Testing** are also deployment controls because technical testing identifies exploitable weaknesses, configuration flaws, and security defects in the release candidate or production-like environment before go-live. Results support remediation decisions and provide evidence for the authorization decision.

**Risk Adjustments** are necessary at deployment because the system's actual implementation, operating environment, interfaces, threat exposure, and residual vulnerabilities may differ from earlier design assumptions. Updating the risk assessment and treatment decisions ensures that risk is understood and formally accepted, mitigated, transferred, or avoided before operational use. NIST describes authorization as a senior official's risk-based decision to allow operation, supported by control assessment and risk information. See NIST SP 800-37 Rev. 2 and NIST SP 800-115.

## QUESTION NO: 4

Which of the following professionals plays the role of a monitor and takes part in the organization's configuration management process

**A.** Chief Information Officer

**B.** Authorizing Official

**C.** Common Control Provider

**D.** Senior Agency Information Security Officer

## ANSWER: C

**Explanation:**

The **Common Control Provider** is the appropriate role because this official is responsible for implementing, assessing, and monitoring controls that are inherited by multiple systems across an organization. Common controls may include enterprise-wide policies, physical safeguards, personnel-security processes, network protections, or centralized identity services. Since a change to one of these shared controls can affect every system that inherits it, the provider must maintain awareness of the control's implementation status and ongoing effectiveness.

NIST's Risk Management Framework assigns the Common Control Provider responsibilities for ensuring that common controls are assessed and monitored, and for making the resulting control information available to system owners and authorizing officials. The role also participates in the organization's configuration-management process so that proposed or implemented changes to common controls are evaluated, documented, and communicated. This monitoring and configuration-management participation supports continuous monitoring, preserves the accuracy of authorization information, and helps ensure that systems relying on inherited controls retain an appropriate security posture. See NIST SP

800-37 Rev. 2, Appendix D, Risk Management Framework for Information Systems and Organizations, and NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations.

## QUESTION NO: 5

Which of the following statements define the role of the ISSEP during the development of the detailed security design, as mentioned in the IATF document Each correct answer represents a complete solution. Choose all that apply.

**A.** It identifies the information protection problems that needs to be solved.

**B.** It allocates security mechanisms to system security design elements.

**C.** It identifies custom security products.

**D.** It identifies candidate commercial off-the-shelf (COTS)government off-the-shelf (GOTS) security products.

## ANSWER: B C D

**Explanation:**

During detailed security design, the ISSEP translates the selected security architecture and requirements into implementable system-design decisions. “It allocates security mechanisms to system security design elements” is correct because this work assigns protections—such as identification and authentication, access enforcement, audit, cryptographic protections, and boundary defenses—to the components, interfaces, and services that will provide them. This allocation creates traceability from security needs to an implementable design.

“It identifies custom security products” and “It identifies candidate commercial off-the-shelf (COTS)government off-the-shelf (GOTS) security products” are also correct because detailed design must determine how the allocated mechanisms will actually be realized. The ISSEP evaluates feasible product and component choices, including available commercial or government solutions as well as the need for purpose-built security capabilities. Product identification supports engineering trade-offs involving assurance, interoperability, integration constraints, lifecycle support, and residual risk. This is consistent with systems security engineering guidance, which treats the allocation of security requirements to system elements and the selection or development of solution components as core design activities. See NIST SP 800-160, Systems Security Engineering and NSA Information Assurance Technical Framework information.

## QUESTION NO: 6

Which of the following types of cryptography defined by FIPS 185 describes a cryptographic algorithm or a tool accepted by the National Security Agency for protecting classified information

**A.** Type III cryptography

**B.** Type III (E) cryptography

**C.** Type II cryptography

**D.** Type I cryptography

## ANSWER: D

**Explanation:**

Type I cryptography is correct because it denotes cryptographic equipment, components, or algorithms that the National Security Agency has classified or certified for protecting classified national-security information. This designation is associated with systems used to protect information at classified levels and is subject to NSA-controlled design, evaluation, production, distribution, and use requirements. In the terminology referenced by FIPS 185, Type I cryptography is specifically the category appropriate to classified information, rather than merely sensitive but unclassified information or commercial applications.

FIPS 185, the Escrowed Encryption Standard, includes the relevant terminology and identifies Type I products as those classified or certified by NSA for the protection of classified or sensitive U.S. Government information, depending on the

system's approved use. The key point in the question is NSA acceptance for protecting *classified* information, which directly identifies the Type I designation. See the original NIST FIPS 185 publication and NSA's overview of national-security cryptography.

## QUESTION NO: 7 - (SIMULATION)

SIMULATION

For interactive and self-paced preparation of exam ISSEP, try our practice exams.

Practice exams also include self assessment and reporting features!

Fill in the blank with an appropriate word. _____ has the goal to securely interconnect people and systems independent of time or location.

## ANSWER: See the explanation for the answer

**Explanation:**

**Answer:** `Network-centric operations (NCO)`

Network-centric operations aim to securely interconnect people, information, and systems so they can communicate and collaborate regardless of time or location.

## QUESTION NO: 8

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.** CA Certification, Accreditation, and Security Assessments

**B.** Information systems acquisition, development, and maintenance

**C.** IR Incident Response

**D.** SA System and Services Acquisition

## ANSWER: A C D

**Explanation:**

The U.S. federal information-security control framework is defined principally through NIST publications used to support FISMA implementation. "CA Certification, Accreditation, and Security Assessments," "IR Incident Response," and "SA System and Services Acquisition" correspond to NIST SP 800-53 control families. These families organize security and privacy requirements that federal agencies select, tailor, implement, assess, authorize, and continuously monitor for their information systems.

Certification and accreditation terminology reflects the earlier authorization approach used in federal guidance; the current NIST SP 800-53 family is titled Assessment, Authorization, and Monitoring, while retaining the same essential federal governance purpose of evaluating controls and supporting an authorization decision. Incident Response establishes requirements for preparing for, detecting, analyzing, containing, recovering from, and reporting cybersecurity incidents. System and Services Acquisition addresses integrating security requirements into the system-development life cycle and into externally provided systems and services. Together, these are recognized federal control-family areas rather than merely general security-practice topics. NIST's control catalog is available in NIST SP 800-53 Rev. 5, and the federal statutory risk-management context is summarized by NIST's FISMA background.

## QUESTION NO: 9

Fill in the blank with the appropriate phrase. _____ provides instructions and directions for completing the Systems Security Authorization Agreement (SSAA).

**A.** DITSCAP Application Manual (DIAM)

**ANSWER: A**

**Explanation:**

The **DITSCAP Application Manual (DIAM)** provides the instructions and direction for preparing and completing the Systems Security Authorization Agreement (SSAA). The SSAA was the principal agreement and authorization documentation used under the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP). It recorded the system's security requirements, certification activities, risk-related decisions, operational environment, and the commitments of the involved stakeholders. The DIAM supplied the practical implementation guidance needed to develop that agreement consistently, including how the SSAA is structured, maintained, reviewed, and used throughout the accreditation effort. This makes the manual—not merely the general DITSCAP policy—the appropriate phrase for a statement specifically asking what provides completion instructions and directions for the SSAA. DITSCAP and its SSAA documentation are historical predecessors to the current Department of Defense Risk Management Framework authorization approach. The original manual is available through the Defense Technical Information Center. For current authorization concepts and terminology, see NIST SP 800-37 Rev. 2.

**QUESTION NO: 10**

Which of the following DoD policies establishes IA controls for information systems according to the Mission Assurance Categories (MAC) and confidentiality levels

**A.** DoD 8500.1 Information Assurance (IA)

**B.** DoD 8500.2 Information Assurance Implementation

**C.** DoDI 5200.40

**D.** DoD 8510.1-M DITSCAP

**ANSWER: B**

**Explanation:**

**DoD 8500.2 Information Assurance Implementation** is correct because it was the DoD instruction that operationalized the Department's information assurance policy by defining specific IA controls and assigning them according to an information system's Mission Assurance Category and confidentiality level. The MAC designation expressed the importance of system availability and integrity to the mission, while the confidentiality level reflected the sensitivity or classification of information handled by the system. Combining those values produced a baseline control set that system owners and authorization personnel could use to implement, assess, and accredit protections consistently across DoD systems. The instruction's control-based approach therefore directly matches the question's reference to establishing IA controls according to MAC and confidentiality levels. This is a legacy DoD IA framework: DoD 8500.2 has since been cancelled and replaced as DoD transitioned to the Risk Management Framework, but it remains the historically accurate answer for terminology centered on MACs and confidentiality levels. See the archived DoD Instruction 8500.2, Information Assurance Implementation and the current DoD Instruction 8510.01, Risk Management Framework for DoD Systems.

**QUESTION NO: 11**

Which of the following Net-Centric Data Strategy goals are required to increase enterprise and community data over private user and system data Each correct answer represents a complete solution. Choose all that apply.

**A.** Understandability

**B.** Visibility

**C.** Interoperability

**D.** Accessibility

**ANSWER: A B C D**

**Explanation:**

The Net-Centric Data Strategy establishes that Department of Defense data should be managed and exposed as an enterprise resource rather than being retained solely within individual applications, systems, or user communities. This objective depends on data being visible, accessible, understandable, and interoperable. Visibility enables potential consumers to discover that data exists through metadata and cataloging. Accessibility permits authorized users and services to retrieve or use the discovered data through appropriate interfaces and controls. Understandability ensures that consumers can interpret the data correctly, including its meaning, structure, context, and intended use. Interoperability enables data to be exchanged and used effectively across different systems, organizations, and mission communities. Together, these characteristics support enterprise-wide and community-wide reuse while preserving required security, access-control, and governance protections. The broader strategy also identifies data trustworthiness as an important attribute, but it is not among the choices presented. This approach is consistent with the DoD instruction governing data sharing in a net-centric environment and with the DoD enterprise data strategy's emphasis on making data discoverable, usable, and shareable across mission partners. See DoDI 8320.02, Sharing Data, Information, and Information Technology Services in the Department of Defense and the DoD Data Strategy.

**QUESTION NO: 12**

Which of the following agencies is responsible for funding the development of many technologies such as computer networking, as well as NLS

**A.** DARPA

**B.** DTIC

**C.** DISA

**D.** DIAP

**ANSWER: A**

**Explanation:**

DARPA is correct because the Defense Advanced Research Projects Agency was the U.S. Department of Defense research-funding organization that sponsored foundational computing and networking work. Through its Information Processing Techniques Office, DARPA funded the ARPANET program, whose packet-switching network research became a major technical and organizational precursor to today's Internet. DARPA's role was not limited to networking: it also supported pioneering interactive-computing research, including work associated with Douglas Engelbart's oN-Line System (NLS) at the Stanford Research Institute's Augmentation Research Center. NLS demonstrated influential concepts and technologies such as interactive hypertext, collaborative computing, screen-based document editing, and use of the computer mouse. These investments reflected DARPA's mission of advancing high-impact, often long-range technologies with potential national-security value. The agency's historical ARPANET materials describe its sponsorship of the network's development and operation, while the Engelbart Institute documents the NLS demonstration and its significance in modern computing history. See DARPA's ARPANET timeline and the Engelbart Institute's NLS history.

**QUESTION NO: 13**

Which of the following elements are normally required to construct a convincing security assurance case for a system Each correct answer represents a complete solution. Choose all that apply.

**A.** Claims

**B.** Arguments

**C.** Evidence

**D.** Risk register

**ANSWER: A B C**

**Explanation:**

A security assurance case is a structured, evidence-based justification that a system is sufficiently trustworthy for its intended use. **Claims** state what is asserted about the system, such as the claim that a security objective or requirement has been satisfied. **Arguments** explain the reasoning that connects the available evidence to the claim. **Evidence** consists of objective artifacts such as test results, analyses, inspection records, assessment findings, design records, and configuration data that support the argument.

The assurance case must also account for assumptions, limitations, and residual risks where they affect the validity of the claims. A risk register can provide useful supporting information, but it is not, by itself, one of the fundamental claim-argument-evidence elements of an assurance case. NIST describes assurance as grounds for confidence that a system meets its security requirements and discusses the role of evidence in systems security engineering in NIST SP 800-160, Volume 1.

## QUESTION NO: 14 - (SIMULATION)

SIMULATION

Fill in the blank with an appropriate phrase. A _____ is defined as any activity that has an effect on defining, designing, building, or executing a task, requirement, or procedure.

**ANSWER: See the explanation for the answer**

**Explanation:**

**Answer:** `process`

A **process** is an activity (or related set of activities) that affects how a task, requirement, or procedure is defined, designed, built, or executed.

## QUESTION NO: 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 activities related to the disposition of the system data and objects.

**B.** Combine validation results in DIACAP scorecard.

**C.** Conduct validation activities.

**D.** Execute and update IA implementation plan.

**ANSWER: B C D**

**Explanation:**

The Implement and Validate Assigned IA Controls phase is where the system owner and supporting security personnel put the planned information-assurance controls into operation and obtain evidence that those controls have been implemented as intended. “Execute and update IA implementation plan” is a subordinate task because the implementation plan is the working record used to track assigned controls, implementation status, resources, milestones, and changes discovered during execution. It must be maintained as the system and its control implementation mature.

“Conduct validation activities” is also central to this phase. Validation produces the evidence needed to determine whether the assigned controls have been implemented correctly and whether they provide the expected protection. This includes

reviewing implementation artifacts, examining configurations, interviewing responsible personnel, and performing testing or assessment procedures as appropriate.

“Combine validation results in DIACAP scorecard” completes the phase’s reporting purpose. The DIACAP scorecard consolidates validation evidence and control status into decision-support information for the accreditation process, including the resulting residual-risk picture. DIACAP is a legacy DoD process that was superseded by the DoD Risk Management Framework, but these tasks describe its historical workflow. See DoD Instruction 8510.01 and NIST SP 800-37 Rev. 2.

## QUESTION NO: 16

Which of the following verification methods can be used to establish that a security requirement has been satisfied by a system implementation Each correct answer represents a complete solution. Choose all that apply.

**A.** Inspection

**B.** Analysis

**C.** Demonstration

**D.** Test

**E.** Risk acceptance

## ANSWER: A B C D

**Explanation:**

**Inspection**, **analysis**, **demonstration**, and **test** are recognized verification methods. Inspection establishes compliance by examining products such as documentation, source code, configurations, labels, or physical components. Analysis uses logical, mathematical, or technical evaluation of evidence to determine whether the requirement has been met. Demonstration establishes that a capability can be performed under specified conditions, while testing uses controlled inputs and expected results to measure whether the implemented system behaves as required.

The selected verification method must be appropriate to the nature of the security requirement and must provide objective evidence for the verification record. For example, an access-control policy may be inspected, a cryptographic design may be analyzed, a failover capability may be demonstrated, and audit-event generation may be tested. Systems security engineering guidance emphasizes planning verification activities and maintaining evidence that requirements have been satisfied. See NIST SP 800-160, Volume 1 and ISO/IEC/IEEE 12207.

## QUESTION NO: 17

Which of the following are the most important tasks of the Information Management Plan (IMP) Each correct answer represents a complete solution. Choose all that apply.

**A.** Define the Information Protection Policy (IPP).

**B.** Define the System Security Requirements.

**C.** Define the mission need.

**D.** Identify how the organization manages its information.

## ANSWER: A C D

**Explanation:**

An Information Management Plan (IMP) establishes the organizational context for handling information throughout a system’s life cycle. “Define the mission need” is essential because the mission establishes why information is collected, created, used, shared, retained, and protected. Understanding that operational purpose allows security engineering activities to align protection decisions with mission success and risk tolerance.

“Define the Information Protection Policy (IPP)” is also a central IMP activity because the plan must establish the policy direction governing appropriate information handling and protection. The policy provides the management-level basis for applying protection expectations consistently across information and associated systems.

“Identify how the organization manages its information” is fundamental to the plan as well. This includes determining information ownership, handling practices, access and distribution needs, storage, lifecycle controls, retention, and disposal expectations. These management arrangements provide the practical structure needed to ensure information remains available, reliable, and appropriately protected in support of the mission. NIST describes systems security engineering as an integrated life-cycle activity that addresses mission and business needs, risk, and protection requirements; see NIST SP 800-160, Volume 1. NIST’s security planning guidance also emphasizes documenting management, operational, and technical controls and responsibilities; see NIST SP 800-18 Rev. 1.

## QUESTION NO: 18

Which of the following DITSCAP C&A phases takes place between the signing of the initial version of the SSAA and the formal accreditation of the system

**A.** Phase 3

**B.** Phase 2

**C.** Phase 4

**D.** Phase 1

## ANSWER: B

**Explanation:**

Phase 2 is correct. In the legacy DoD Information Technology Security Certification and Accreditation Process (DITSCAP), Phase 2 is the Verification phase. It begins after the initial System Security Authorization Agreement (SSAA) has been agreed to and signed by the designated DITSCAP principals. The SSAA establishes the system’s security requirements, the planned certification activities, the acceptable level of residual risk, assigned responsibilities, and the evidence needed to support an accreditation decision.

During Verification, the system is evaluated against the agreed security requirements. Activities include reviewing the system’s security design and documentation, performing security test and evaluation work, assessing implemented safeguards, recording findings, and updating the SSAA and supporting certification evidence as necessary. The resulting certification package provides the accreditation authority with the technical risk information needed to make the formal accreditation decision. Accordingly, this phase occupies the interval after the initial SSAA is signed and before the system receives formal accreditation. DITSCAP is a legacy process that was later superseded within DoD by the Risk Management Framework, but its four-phase terminology remains relevant to historical C&A questions. See the DoD DITSCAP Application Manual and the NIST Risk Management Framework guidance.

## QUESTION NO: 19

Fill in the blank with an appropriate phrase. A _____ is defined as any activity that has an effect on defining, designing, building, or executing a task, requirement, or procedure.

**A.** Security-relevant activity

## ANSWER: A

**Explanation:**

**Security-relevant activity** correctly completes the definition. In systems security engineering, security must be considered wherever work can shape how a system is specified, designed, implemented, operated, or governed. A security-relevant activity is therefore not limited to an explicitly technical security task, such as configuring access controls. It includes any activity whose decisions, outputs, procedures, or execution can influence the security properties of the system or the

assurance that those properties are achieved. This broad interpretation supports early and continuous security integration throughout the system life cycle, rather than treating security as a separate late-stage review.

NIST's systems security engineering guidance emphasizes applying security engineering across system life-cycle processes and technical activities, including requirements, architecture, design, implementation, integration, and operation. This use of security-relevant activities helps ensure that security considerations are incorporated wherever system decisions are made. See NIST SP 800-160, Volume 1 and the NIST Computer Security Resource Center Glossary.

## QUESTION NO: 20

Which of the following DITSCAPNIACAP model phases is used to confirm that the evolving system development and integration complies with the agreements between role players documented in the first phase

**A.** Verification

**B.** Validation

**C.** Post accreditation

**D.** Definition

## ANSWER: A

**Explanation:**

Verification is correct. In the legacy DITSCAP/NIACAP lifecycle, the Definition phase establishes the system security agreement among the key participants, including the system sponsor, program manager, designated approving authority, certifier, and user representative. That agreement records the intended security approach, responsibilities, milestones, required evidence, and the level of effort expected for certification and accreditation activities. The Verification phase then provides the structured, continuing review of the evolving system as it is developed and integrated. Its purpose is to determine whether the implementation, integration activities, and security work remain consistent with the agreements and planned approach established during Definition. This allows participants to identify departures early, resolve them through the established management process, and preserve the evidence needed for the subsequent accreditation decision. Thus, the wording "confirm that the evolving system development and integration complies with the agreements" directly describes verification against the agreed security and engineering baseline, rather than the initial agreement-making activity itself. DITSCAP is a legacy DoD process that preceded the current Risk Management Framework, but its lifecycle terminology remains relevant when answering historical NIACAP/DITSCAP questions. See the DITSCAP Application Manual and NIST's Risk Management Framework publication for lifecycle-oriented security assessment context.

## QUESTION NO: 21

Continuous Monitoring is the fourth phase of the security certification and accreditation process. What activities are performed in the Continuous Monitoring process Each correct answer represents a complete solution. Choose all that apply.

**A.** Status reporting and documentation

**B.** Security control monitoring and impact analyses of changes to the information system

**C.** Configuration management and control

**D.** Security accreditation documentation E. Security accreditation decision

## ANSWER: A B C

**Explanation:**

Continuous Monitoring maintains the security authorization decision by providing ongoing awareness of security-control effectiveness and of changes that could alter the system's risk posture. **Status reporting and documentation** is an essential activity because authorization officials and other risk-management stakeholders need current, documented information about monitoring results, control status, vulnerabilities, and risk. **Security control monitoring and impact**

**analyses of changes to the information system** is also central: organizations assess selected controls at defined frequencies and analyze proposed or implemented changes to determine their security effect before accepting the resulting risk. **Configuration management and control** supports this process by ensuring that system modifications are identified, evaluated, authorized, implemented, and tracked in a disciplined manner. Together, these activities preserve an accurate understanding of the authorized system configuration and enable timely risk-based decisions throughout the system life cycle. NIST describes continuous monitoring as maintaining ongoing situational awareness of security and privacy control effectiveness, system changes, and risk. See NIST SP 800-37 Rev. 2 and NIST SP 800-137.

## QUESTION NO: 22

What are the responsibilities of a system owner Each correct answer represents a complete solution. Choose all that apply.

**A.** Integrates security considerations into application and system purchasing decisions and development projects.

**B.** Ensures that the necessary security controls are in place.

**C.** Ensures that adequate security is being provided by the necessary controls, password management, remote access controls, operating system configurations, and so on.

**D.** Ensures that the systems are properly assessed for vulnerabilities and must report any to the incident response team and data owner.

## ANSWER: A B D

**Explanation:**

A system owner is accountable for the system throughout its life cycle, including its acquisition, development, integration, operation, maintenance, and eventual disposal. Consequently, integrating security considerations into application and system purchasing decisions and development projects is a core system-owner responsibility. The system owner must also ensure that the system has the necessary security controls implemented and that those controls support the system's required security posture. This accountability does not mean personally performing every technical configuration task; rather, the owner ensures that appropriate resources, processes, and responsible personnel are in place.

System owners are also responsible for ensuring that security assessments occur as required and that identified vulnerabilities receive appropriate visibility and handling. Reporting significant vulnerability information to relevant incident-response personnel and the data owner supports risk decisions, remediation prioritization, and protection of the information processed by the system. NIST defines the system owner as the organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system, and assigns responsibility for ensuring that security controls are implemented and assessed. See NIST SP 800-37 Rev. 2 and NIST SP 800-18 Rev. 1.

## QUESTION NO: 23

According to which of the following DoD policies, the implementation of DITSCAP is mandatory for all the systems that process both DoD classified and unclassified information?

**A.** DoD 8500.2

**B.** DoDI 5200.40

**C.** DoD 8510.1-M DITSCAP

**D.** DoD 8500.1 (IAW)

## ANSWER: D

**Explanation:**

DoD 8500.1 (IAW) is correct because DoD Directive 8500.1, *Information Assurance (IA)*, established the Department-wide information-assurance policy framework under which the DoD Information Technology Security Certification and

Accreditation Process (DITSCAP) was required. The directive required DoD IT systems to use DITSCAP to manage information-assurance activities throughout a system's acquisition, operation, and sustainment life cycle. Its scope included systems handling both classified and unclassified DoD information, making it the policy-level authority for the mandatory use described in the question.

DITSCAP was the historical DoD certification-and-accreditation process intended to provide decision makers with a structured basis for accepting residual risk and authorizing system operation. Although DoD has since transitioned from DITSCAP and DIACAP to the Risk Management Framework, the question uses the terminology and policy structure in effect when DoD 8500.1 governed this requirement. The current DoD RMF policy is documented in DoD Instruction 8510.01; DoD directive issuances, including the 8500-series cybersecurity policy lineage, are maintained through the Washington Headquarters Services DoD Issuances portal.

## QUESTION NO: 24

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.** Initiation

**B.** Security Certification

**C.** Continuous Monitoring

**D.** Security Accreditation

## ANSWER: D

**Explanation:**

**Security Accreditation** is correct. In the former NIST Special Publication 800-37 certification-and-accreditation process, this phase is the formal authorization decision activity performed by the authorizing official. It considers the security certification results, the documented plan of action and milestones, and the resulting residual risk to determine whether that risk is acceptable for the system's intended operation. The accreditation package supplies the evidence needed for this decision, including the security plan, security assessment or certification documentation, and remediation information. If the risk is accepted, the authorizing official grants an accreditation (authorization to operate); if it is not acceptable, the official may require corrective actions, issue an interim authorization with conditions, or deny authorization. This risk-based executive decision is central to the accreditation phase because system owners and technical assessors provide assessment evidence, while the authorizing official explicitly accepts accountability for the remaining risk. NIST later transitioned terminology from "accreditation" to "authorization" under the Risk Management Framework, but the underlying purpose remains the same: an accountable official evaluates residual risk and makes the final operational authorization decision. See NIST SP 800-37 Rev. 1 and NIST's Authorization to Operate glossary entry.

## QUESTION NO: 25

Which of the following principles are defined by the IATF model Each correct answer represents a complete solution. Choose all that apply.

**A.** The degree to which the security of the system, as it is defined, designed, and implemented, meets the security needs.

**B.** The problem space is defined by the customer's mission or business needs.

**C.** The systems engineer and information systems security engineer define the solution space, which is driven by the problem space.

**D.** Always keep the problem and solution spaces separate.

## ANSWER: B C D

**Explanation:**

The IATF security engineering model distinguishes the customer's problem space from the engineering solution space. "The problem space is defined by the customer's mission or business needs" is a core principle because mission and business objectives establish the operational context, needed capabilities, assets, constraints, and protection needs that engineering must address. Security requirements are therefore derived in support of the mission rather than selected independently as a technology-first exercise.

"The systems engineer and information systems security engineer define the solution space, which is driven by the problem space" is also correct. The systems engineer and ISSE collaborate to translate stakeholder needs and security needs into an implementable system solution, including security architecture, requirements, mechanisms, and assurance evidence. This preserves traceability from mission needs through system requirements and design decisions.

"Always keep the problem and solution spaces separate" expresses the necessary conceptual separation between identifying what must be accomplished and deciding how it will be accomplished. Keeping these spaces distinct helps prevent prematurely constraining the design, while allowing the resulting solution to remain demonstrably responsive to mission-driven requirements. This approach aligns with the systems-security-engineering life-cycle concepts in NIST SP 800-160, Systems Security Engineering and the ISSEP domain expectations described in the ISC2 ISSEP Exam Outline.

## QUESTION NO: 26

You work as a system engineer for BlueWell Inc. Which of the following documents will help you to describe the detailed plans, procedures, and schedules to guide the transition process

**A.** Configuration management plan

**B.** Transition plan

**C.** Systems engineering management plan (SEMP)

**D.** Acquisition plan

## ANSWER: B

**Explanation:**

**Transition plan** is correct because it documents how a system, service, capability, or operational responsibility will move from its current state into the target operational environment. It provides the actionable detail needed to manage that move safely and predictably, including the transition approach, implementation activities, sequencing, schedules, assigned responsibilities, required resources, dependencies, communication and training activities, readiness criteria, testing or validation steps, fallback procedures, and post-transition support. In systems engineering, transition planning turns a solution that has been developed and verified into one that can be deployed, accepted, operated, and sustained by its intended users and operational organization. The plan therefore serves as the practical guide for coordinating stakeholders and controlling risk throughout deployment or handover. This use is consistent with NIST system-development guidance, which treats implementation and transition activities as planned work required to put a system into operation, and with the NASA systems engineering framework's treatment of product transition as the process of preparing and transferring a product to its operational environment. See NIST SP 800-64 Rev. 2 and NASA Systems Engineering Handbook.