DUMPSHQ

Free Questions for ISSEP by dumpshq

Shared by Ortiz on 09-08-2024

Question 1

Question Type: **MultipleChoice**

Which of the following guidelines is recommended for engineering, protecting, managing, processing, and controlling national security and sensitive (although unclassified) information?

Options:

A) Federal Information Processing Standard (FIPS)

B) Special Publication (SP)

C) NISTIRs (Internal Reports)

D) DIACAP by the United States Department of Defense (DoD)

Answer:

B

Explanation:

The Special Publication (SP) is the guideline that is recommended for engineering, protecting, managing, processing, and controlling national security and sensitive (although unclassified) information. Answer option D is incorrect. The Department of Defense Information Assurance

Certification and Accreditation Process (DIACAP) is a process defined by the United States

Department of Defense (DoD) for managing risk. DIACAP replaced the former process, known as

DITSCAP (Department of Defense Information Technology Security Certification and Accreditation

Process), in 2006. DoD Instruction (DoDI) 8510.01 establishes a standard DoD-wide process with a

set of activities, general tasks, and a management structure to certify and accredit an Automated

Information System (AIS) that will maintain the Information Assurance (IA) posture of the Defense

Information Infrastructure (DII) throughout the system's life cycle. The DIACAP process is different

from DITSCAP or NIACAP. Its overall process is similar to other C&amp;A activities. The DIACAP process

consists of five phases, which are as follows:

1.Initiate and Plan IA C&amp;A. This phase consists of the following activities:

Register system with DoD Component IA Program.

Assign IA controls.

Assemble DIACAP team.

Develop DIACAP strategy.

Initiate IA implementation plan.

2.Implement and Validate Assigned IA Controls: This phase consists of the following activities:

Execute and update IA implementation plan. Conduct validation activities. Combine validation

results in DIACAP scorecard. 3.Make Certification Determination and Accreditation Decisions: This

phase consists of the following activities:

Analyze residual risk.Issue certification determination.Make accreditation decision.

4.Maintain Authority to Operate and Conduct Reviews: This phase consists of the following activities:

Initiate and update lifecycle implementation plan for IA controls.

Maintain situational awareness.Maintain IA posture.

5.Decommission System: This phase consists of the following activities:

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

Answer option A is incorrect. FIPS emphasizes on design, implementation, and approval of

cryptographic algorithms.Answer option C is incorrect. NISTIRs (Internal Reports) illustrate the study of a technical nature of interest to focused audience. NISTIRs consist of interim or final reports on work made by NIST for external sponsors, including government and non-government sponsors.

Question 2

Question Type: MultipleChoice

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

Options:

A) Chief Information Officer

B) Authorizing Official

C) Common Control Provider

D) Senior Agency Information Security Officer

Answer:

C

Explanation:

A Common Control Provider plays the role of a monitor. The responsibilities of a Common Control Provider are as follows:

Develops a continuous monitoring scheme for the assigned common controls.

Takes part in the organization's configuration management process.

Establishes a stock of components associated with the common controls.

Performs security impact analysis on the changes that affect the common controls.

Performs security assessments of the common security controls.

Creates and submits security status reports to the defined organizations.

Updates critical security documents and provides it to information system owners and other leaders.

Performs remediation activities to maintain current authorization status.

Answer option A is incorrect. The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the

most senior executive in an enterprise responsible for the information technology and computer systems that support enterprise goals. The CIO plays the role of a leader and reports to the chief executive officer, chief operations officer, or chief financial officer. In military organizations, they report to the commanding officer.

Answer option B is incorrect. An Authorizing Official plays the role of an approver. The responsibilities of an Authorizing Official are as follows:

Ascertains the security posture of the organization's information system.

Reviews security status reports and critical security documents.Determines the requirement of reauthorization and reauthorizes information systems when required.

Answer option D is incorrect. A Senior Agency Information Security Officer plays the role of a coordinator. The responsibilities of a Senior Agency Information Security Officer are as follows:

Establishes and implements the organization's continuous monitoring program.

Develops organizational guidance and configuration guidance for continuous monitoring of information systems and organization's information technologies respectively.

Consolidates and analyzes Plans of Action and Milestones (POAM) to decide organizational security weakness and inadequacy. Develops automated tools to support security authorization and continuous monitoring.Provides training on the organization's continuous monitoring process.

Provides help to information system owners to develop and implement continuous monitoring.

Question 3

Question Type: MultipleChoice

Which of the following Security Control Assessment Tasks gathers the documentation and supporting materials essential for the assessment of the security controls in the information system?

Options:

A) Security Control Assessment Task 4

B) Security Control Assessment Task 3

C) Security Control Assessment Task 1

D) Security Control Assessment Task 2

Answer:

C

Explanation:

Security Control Assessment Task 1 gathers the documentation and supporting materials essential for the assessment of the security controls in the information system.

Answer option D is incorrect. Security Control Assessment Task 2 develops methods and procedures.

Answer option B is incorrect. Security Control Assessment Task 3 evaluates the operational,

technical, and the management security controls of the information system using the techniques and measures selected or developed.

Answer option A is incorrect. Security Control Assessment Task 4 prepares the final security assessment report.

Question 4

Question Type: MultipleChoice

Which of the following processes culminates in an agreement between key players that a system in its current configuration and operation provides adequate protection controls?

Options:

A) Certification and accreditation (C&A)

B) Risk Management

C) Information systems security engineering (ISSE)

D) Information Assurance (IA)

Answer:

A

Explanation:

Certification and accreditation (C&amp;A) is a set of processes that culminate in an agreement between key players that a system in its current configuration and operation provides adequate protection controls.

Certification and Accreditation (C&amp;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&amp;A process is used extensively in the U.S. Federal Government. Some

C&amp;A processes include FISMA, NIACAP, DIACAP, and DCID 6/3.

Certification is a comprehensive assessment of the management, operational, and technical security

controls in an information system, made in support of security accreditation, to determine the

extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

Answer option B is incorrect. Risk management is a set of processes that ensures a risk-based approach is used to determine adequate, cost-effective security for a system.

Answer option D is incorrect. Information assurance (IA) is the process of organizing and monitoring information-related risks. It ensures that only the approved users have access to the approved information at the approved time. IA practitioners seek to protect and defend information and information systems by ensuring confidentiality, integrity, authentication, availability, and non-repudiation. These objectives are applicable whether the information is in storage, processing, or transit, and whether threatened by an attack.

Answer option C is incorrect. ISSE is a set of processes and solutions used during all phases of a system's life cycle to meet the system's information protection needs.

Question 5

Question Type: **MultipleChoice**

Which of the following email lists is written for the technical audiences, and provides weekly summaries of security issues, new vulnerabilities, potential impact, patches and workarounds, as well as the actions recommended to mitigate risk?

Options:

A) Cyber Security Tip

B) Cyber Security Alert

C) Cyber Security Bulletin

D) Technical Cyber Security Alert

Answer:

C

Explanation:

The various free email lists are as follows:

Cyber Security Bulletins: This type of email list is written for the technical audiences. The Cyber Security Bulletins present the weekly summaries of security issues, new vulnerabilities, potential impact, patches and workarounds, and actions recommended mitigating risk.

Technical Cyber Security Alerts: This type of email list is written for the technical audiences. The Cyber Security Alerts give the timely information about current security issues, vulnerabilities, and exploits.

Cyber Security Alerts: This type of email list is written for non-technical home and corporate computer users. The Cyber Security Alerts give the timely information about security issues, vulnerabilities, and exploits currently occurring.

Cyber Security Tips: This type of email list is written for non-technical home and corporate computer users. The bi-weekly Cyber Security Tips gives information on computer security best practices.

Question 6

Question Type: MultipleChoice

The Phase 4 of DITSCAP C&A is known as Post Accreditation. This phase starts after the system has been accredited in Phase 3. What are the process activities of this phase?

Each correct answer represents a complete solution. Choose all that apply.

Options:

A) Security operations

B) Continue to review and refine the SSAA

C) Change management

D) Compliance validation

E) System operations

F) Maintenance of the SSAA

Answer:

A, C, D, E, F

Explanation:

The Phase 4 of DITSCAP C&amp;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

Answer option B is incorrect. It is a Phase 3 activity.

Question 7

Question Type: **MultipleChoice**

Which of the following tasks obtains the customer agreement in planning the technical effort?

Options:

A) Task 9

B) Task 11

C) Task 8

D) Task 10

Answer:

B

Explanation:

The various tasks performed in Plan the Effort process are as follows:

Task 1: Estimate project scope.

Task 2: Identify resources and availability.

Task 3: Identify roles and responsibilities.

Task 4: Estimate project costs.

Task 5: Develop project schedule.

Task 6: Identify technical activities.

Task 7: Identify deliverables.

Task 8: Define management interfaces.

Task 9: Prepare technical management plan.

Task 10: Review project plan.

Task 11: Obtain customer agreement.

Question 8

Question Type: MultipleChoice

Which of the following documents is defined as a source document, which is most useful for the ISSE when classifying the needed security functionality?

Options:

A) Information Protection Policy (IPP)

B) IMM

C) System Security Context

D) CONOPS

Answer:

A

Explanation:

The Information Protection Policy (IPP) is defined as a source document, which is most useful for the ISSE when classifying the needed security functionality. The IPP document consists of the threats to the information management and the security services and controls needed to respond to those threats. Answer option B is incorrect. The IMM is the source document describing the customer's needs based on identifying users, processes, and information. Answer option C is incorrect. The System Security Context is the output of SE and ISSEP. It is the translation of the requirements into system parameters and possible measurement concepts that meet the defined requirements. Answer option D is incorrect. The Concept of Operations (CONOPS) is a document describing the characteristics of a proposed system from the viewpoint of an individual who will use that system. It is used to communicate the quantitative and qualitative system characteristics to all stakeholders. CONOPS are widely used in the military or in government services, as well as other fields. A CONOPS generally evolves from a concept and is a description of how a set of capabilities may be employed to achieve desired objectives or a particular end state for a specific scenario.

Question 9

Question Type: MultipleChoice

Which of the following elements are described by the functional requirements task?

Each correct answer represents a complete solution. Choose all that apply.

Options:

A) Coverage

B) Accuracy

C) Quality

D) Quantity

Answer:

A, C, D

Explanation:

The functional requirements categorize the different functions that the system will need to perform in order to gather the documented mission/business needs. The functional requirements describe the elements such as quantity, quality, coverage, timelines, and availability. Answer option B is incorrect. The performance requirements comprise of speed, throughput, accuracy, humidity tolerances, mechanical stresses such as vibrations or noises.

Question 10

Question Type: MultipleChoice

Which of the following Registration Tasks sets up the business or operational functional description and system identification?

Options:

A) Registration Task 2

B) Registration Task 1

C) Registration Task 3

D) Registration Task 4

Answer:

B

Explanation:

Registration Task 1 sets up the business or operational functional description and system identification.

Answer option D is incorrect. Registration Task 4 sets up the system architecture description, and describes the C&amp;A boundary.

Answer option A is incorrect. Registration Task 2 notifies the DAA, Certifier, and User Representative that the system requires C&amp;A support.

Answer option C is incorrect. Registration Task 3 sets up the environment and threat description.