Free Questions for ISSEP by vceexamstest

Shared by Osborn on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following characteristics are described by the DIAP Information Readiness Assessment function? Each correct answer represents a complete solution. Choose all that apply.

Options:

A- It performs vulnerability/threat analysis assessment.

B- It provides for entry and storage of individual system data.

C- It provides data needed to accurately assess IA readiness.

D- It identifies and generates IA requirements.

Answer:

A, C, D

Explanation:

The characteristics of the DIAP Information Readiness Assessment function are as follows :

It provides data needed to accurately assess IA readiness.

It identifies and generates IA requirements.

It performs vulnerability/threat analysis assessment.

Answer option B is incorrect. It is a function performed by the ASSET system.

Question 2

Question Type: MultipleChoice

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 sensitive, unclassified

information in the systems as stated in Section 2315 of Title 10, United States Code?

Options:

A- Type I cryptography

B- Type II cryptography

C- Type III (E) cryptography

D- Type III cryptography

Answer:

B

Explanation:

The types of cryptography defined by FIPS 185 are as follows:

Type I cryptography: It describes a cryptographic algorithm or a tool accepted by the National

Security Agency for protecting classified information.

Type II cryptography: It describes a cryptographic algorithm or a tool accepted by the National

Security Agency for protecting

sensitive, unclassified information in the systems as stated in Section 2315 of Title 10, United States

Code, or Section 3502(2) of Title 44, United States Code.

Type III cryptography: It describes a cryptographic algorithm or a tool accepted as a Federal

Information Processing Standard.

Type III (E) cryptography: It describes a Type III algorithm or a tool that is accepted for export from the United States.

Question 3

Question Type: MultipleChoice

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.

Options:

A- Providing IA Certification and Accreditation

B- Providing command and control and situational awareness

C- Defending systems

D- Protecting information

Answer:

B, C, D

Explanation:

The various objectives of the DoD 8500 series are as follows:

Protecting information

Defending systems

Providing command and control and situational awareness

Making sure that the information assurance is integrated into processes

Increasing security awareness throughout the DoD's workforce

Question 4

Question Type: **MultipleChoice**

Which of the following cooperative programs carried out by NIST speed ups the development of modern technologies for broad, national benefit by co-funding research and development partnerships with the private sector?

Options:

A- Baldrige National Quality Program

B- Advanced Technology Program

C- Manufacturing Extension Partnership

D- NIST Laboratories

Answer:

B

Explanation:

The cooperative programs carried out by NIST are as follows:

NIST Laboratories: This program conducts research to advance the nation's technology

infrastructure.

Baldrige National Quality Program: This program encourages performance excellence among U.S. manufacturers, service companies, educational institutions, and healthcare providers. It helps to administer the annual Malcolm Baldrige National Quality Award, which recognizes performance excellence and quality achievement.

Manufacturing Extension Partnership: This program provides a nationwide network of local centers offering technical and business assistance to small manufacturers.

Advanced Technology Program: This program speeds up the development of modern technologies for broad, national benefit by co-funding research and development partnerships with the private sector.

Question 5

Question Type: **MultipleChoice**

Which of the CNSS policies describes the national policy on certification and accreditation of national security telecommunications and information systems?

Options:

A- NSTISSP No. 7

B- NSTISSP No. 11

C- NSTISSP No. 6

D- NSTISSP No. 101

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 6

Question Type: **FillInTheBlank**

Fill in the blanks with an appropriate phrase.

The_____ is the process of translating system requirements into detailed function criteria.

Answer:

Explanation:

comprehensive function standard. Verification

is the result of the functional analysis process, in which the fundamentals of a system level

functional architecture are defined adequately to

allow for synthesis in the design phase. The functional analysis breaks down the higher-level

functions into the lower level functions.

Question 7

Question Type: MultipleChoice

Della works as a systems engineer for BlueWell Inc. She wants to convert system requirements into a comprehensive function standard, and break the higher-level functions into lower-level functions.

Which of the following processes will Della use to accomplish the task?

Options:

A- Risk analysis

B- Functional allocation

C- Functional analysis

D- Functional baseline

Answer:

C

Explanation:

The functional analysis process is used for converting system requirements into a comprehensive function standard. Verification is the result of

the functional analysis process, in which the fundamentals of a system level functional architecture are defined adequately to allow for synthesis in the design phase. The functional analysis breaks down the higher-level functions into the lower level functions.

Answer option B is incorrect. Functional allocation is the process of allocating performance and design requirements to each function.

Answer option A 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 option D is incorrect. The functional baseline is used as the approved set of documents, which describes the overall system

specifications.

Question 8

Question Type: MultipleChoice

Which of the following describes a residual risk as the risk remaining after a risk mitigation has occurred?

Options:

A- SSAA

B- ISSO

C- DAA

D- DIACAP

Answer:

B

Explanation:

DIACAP describes a residual risk as the risk remaining after a risk mitigation has occurred. 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.

DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects,

stores, transmits, or processes unclassified or

classified information since December 1997. It identifies four phases:

1.System Definition

2.Verification

3.Validation

4.Re-Accreditation

Answer option B is incorrect. An Information System Security Officer (ISSO) plays the role of a supporter. The responsibilities of an Information

System Security Officer (ISSO) are as follows:

Manages the security of the information system that is slated for Certification & Accreditation (C&A).

Insures the information systems configuration with the agency's information security policy.

Supports the information system owner/information owner for the completion of security-related responsibilities.

Takes part in the formal configuration management process.

Prepares Certification & Accreditation (C&A) packages.

Answer option C is incorrect. The Designated Approving Authority (DAA), in the United States Department of Defense, is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. The DAA is responsible for implementing system security. The DAA can grant the accreditation and can determine that the system's risks are not at an acceptable level and the system is not ready to be operational.

Answer option A is incorrect. System Security Authorization Agreement (SSAA) is an information security document used in the United States Department of Defense (DoD) to describe and accredit networks and systems. The SSAA is part of the Department of Defense Information Technology Security Certification and Accreditation Process, or DITSCAP (superseded by DIACAP). The DoD instruction (issues in December 1997, that describes DITSCAP and provides an outline for the SSAA document is DODI 5200.40. The DITSCAP application manual (DoD 8510.1-

M), published in July 2000, provides additional details.

Question 9

Question Type: MultipleChoice

Which of the following organizations assists the President in overseeing the preparation of the

federal budget and to supervise its administration in Executive Branch agencies?

Options:

A- NSA/CSS

B- OMB

C- DCAA

D- NIST

Answer:

B

Explanation:

The Office of Management and Budget (OMB) is a Cabinet-level office, and is the largest office within the Executive Office of the President (EOP) of the United States. The current OMB Director is Peter Orszag and was appointed by President Barack Obama.

The OMB's predominant mission is to assist the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies. In helping to formulate the President's spending plans, the OMB evaluates the effectiveness of agency programs, policies, and procedures, assesses competing funding demands among agencies, and sets funding priorities. The OMB ensures that agency reports, rules, testimony, and proposed legislation are consistent with the President's Budget and with Administration policies. Answer option C is incorrect. The DCAA has the aim to monitor contractor costs and perform contractor audits.

Answer option A is incorrect. The National Security Agency/Central Security Service (NSA/CSS) is a crypto-logic intelligence agency of the United States government. It is administered as part of the United States Department of Defense. NSA is responsible for the collection and analysis

of foreign communications and foreign signals intelligence, which involves cryptanalysis.

NSA is also responsible for protecting U.S. government communications and information systems from similar agencies elsewhere, which involves cryptography. NSA is a key component of the U.S. Intelligence Community, which is headed by the Director of National Intelligence.

The Central Security Service is a co-located agency created to coordinate intelligence activities and co-operation between NSA and U.S. military cryptanalysis agencies. NSA's work is limited to communications intelligence. It does not perform field or human intelligence activities.

Answer option D is incorrect. The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science,

standards, and technology in ways that enhance economic security and improve quality of life.