Free Questions for ISSEP by certsinside

Shared by Stuart on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Registration Task 5 identifies the system security requirements. Which of the following elements of Registration Task 5 defines the type of data processed by the system?

Options:

A- Data security requirement

B- Network connection rule

C- Applicable instruction or directive

D- Security concept of operation

Answer:

A

Explanation:

Data security requirement defines the type of data processed by the system.

Answer option C is incorrect. Applicable instruction or directive defines the security instructions or directives applicable to the system.

Answer option D is incorrect. Security concept of operation defines the following elements:

Security CONOPS

System input

System processing

Final outputs

Security controls and interactions

Connections with external systems

Answer option B is incorrect. Network connection rule is used to find the additional requirements incurred if the system is to be connected to

any other network or system.

Question 2

Question Type: **MultipleChoice**

John works as a security engineer for BlueWell Inc. He wants to identify the different functions that the system will need to perform to meet the documented mission/business needs. Which of the following processes will John use to achieve the task?

Options:

A- Modes of operation

B- Performance requirement

C- Functional requirement

D- Technical performance measures

Answer:

C

Explanation:

The Functional requirements are used to classify the different functions that the system will need to

perform to meet the documented

mission/business needs.

Answer option B is incorrect. The Performance requirements are the agreed-upon terms of how well

the system functions.

Answer option A is incorrect. The modes of operation defines the mode, such as training mode, pre-production mode, etc.

Answer option D is incorrect. The Technical performance measures are key indicators of system performance such as key critical measures of effectiveness that will put the project at risk.

Question 3

Question Type: MultipleChoice

Which of the following requires all general support systems and major applications to be fully certified and accredited before these systems and applications are put into production? Each correct answer represents a part of the solution. Choose all that apply.

Options:

A- Office of Management and Budget (OMB)

B- NIST

C- FISMA

D- FIPS

Answer:

A, C

Explanation:

FISMA and Office of Management and Budget (OMB) require all general support systems and major

applications to be fully certified and

accredited before they are put into production. General support systems and major applications are

also referred to as information systems

and are required to be reaccredited every three years.

Answer option B 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.

Answer option D is incorrect. The Federal Information Processing Standards (FIPS) are publicly

announced standards developed by the United

States federal government for use by all non-military government agencies and by government

contractors. Many FIPS standards are modified

Some FIPS standards were originally developed by the U.S. government. For instance, standards for

encoding data (e.g., country codes), but

more significantly some encryption standards, such as the Data Encryption Standard (FIPS 46-3) and

the Advanced Encryption Standard (FIPS

197). In 1994, NOAA (Noaa) began broadcasting coded signals called FIPS (Federal Information

Processing System) codes along with their

standard weather broadcasts from local stations. These codes identify the type of emergency and

the specific geographic area (such as a

county) affected by the emergency.

Question 4

Question Type: MultipleChoice

Which of the following are the benefits of SE as stated by MIL-STD-499B? Each correct answer represents a complete solution. Choose all that apply.

Options:

A- It develops work breakdown structures and statements of work.

B- It establishes and maintains configuration management of the system.

C- It develops needed user training equipment, procedures, and data.

D- It provides high-quality products and services, with the correct people and performance features, at an affordable price, and on time.

Answer:

A, B, C

Explanation:

The benefits of SE as stated by MIL-STD-499B are as follows :

It encompasses the scientific and engineering efforts related to the development, manufacturing,

verification, deployment, operations,

support, and disposal of system products and processes.

It develops needed user training equipment, procedures, and data.

It establishes and maintains configuration management of the system.

It develops work breakdown structures and statements of work.

It provides information for management decision-making.

Answer option D is incorrect. This is the objective of SE as defined by IEEE 1220.

Question 5

Question Type: MultipleChoice

Which of the following types of cryptography defined by FIPS 185 describes a cryptographic algorithm or a tool accepted as a Federal Information Processing Standard?

Options:

A- Type III (E) cryptography

B- Type III cryptography

C- Type I cryptography

D- Type II 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 6

Question Type: **MultipleChoice**

Which of the following are the functional analysis and allocation tools? Each correct answer represents a complete solution. Choose all that apply.

Options:

A- Functional flow block diagram (FFBD)

B- Activity diagram

C- Timeline analysis diagram

D- Functional hierarchy diagram

Answer:

A, C, D

Explanation:

The various functional analysis and allocation tools are as follows:

Functional hierarchy diagram: It models the hierarchy of functions that the system is in charge for

performing, the sub-functions that

are required by those functions, and any business processes that are used to invoke those sub

functions. The objective of functional

hierarchy diagram is to show all of the function requirements and their groupings in one diagram.

Functional flow block diagram (FFBD): The objective of FFBDs is to construct the system

requirements into functional terms. The FFBD

classifies the major system-level (or top-level) functions that must be performed by the system to

accomplish its mission.

Timeline analysis diagram: It presents a graphical view of whether the functions are to be

accomplished in series or in parallel.

Answer option B is incorrect. The activity diagram is not a part of the functional analysis and

allocation tools.

Question 7

Question Type: **MultipleChoice**

Which of the following DoD policies establishes policies and assigns responsibilities to achieve DoD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network-centric warfare?

Options:

A- DoD 8500.2 Information Assurance Implementation

B- DoD 8510.1-M DITSCAP

C- DoDI 5200.40

D- DoD 8500.1 Information Assurance (IA)

Answer:

D

Explanation:

DoD 8500.1 Information Assurance (IA) sets up policies and allots responsibilities to achieve DoD IA

through a defense-in-depth approach that

integrates the capabilities of personnel, operations, and technology, and supports the evolution to

network-centric warfare.

DoD 8500.1 also summarizes the roles and responsibilities for the persons responsible for carrying out the IA policies.

Answer option A is incorrect. The DoD 8500.2 Information Assurance Implementation pursues 8500.1. It provides assistance on how to implement policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks.

DoD Instruction 8500.2 allots tasks and sets procedures for applying integrated layered protection of the DOD information systems and networks in accordance with the DoD 8500.1 policy. It also provides some important guidelines on how to implement an IA program.

Answer option C is incorrect. DoDI 5200.40 executes the policy, assigns responsibilities, and recommends procedures under reference for Certification and Accreditation(C&A) of information technology (IT).

Answer option B is incorrect. DoD 8510.1-M DITSCAP provides standardized activities leading to

accreditation, and establishes a process and

management baseline.

Question 8

Question Type: MultipleChoice

Which of the following laws is the first to implement penalties for the creator of viruses, worms, and other types of malicious code that causes harm to the computer systems?

Options:

A- Computer Fraud and Abuse Act

B- Computer Security Act

C- Gramm-Leach-Bliley Act

D- Digital Millennium Copyright Act

Answer:

A

Explanation:

The Computer Fraud and Abuse Act as amended, provides civil penalties for the creator of viruses,

worms, and other types of malicious code

that causes harm to the computer systems.

The Computer Fraud and Abuse Act is a law passed by the United States Congress in 1984 intended

to reduce cracking of computer systems

and to address federal computer-related offenses. The Computer Fraud and Abuse Act (codified as

18 U.S.C. 1030) governs cases with a

compelling federal interest, where computers of the federal government or certain financial

institutions are involved, where the crime itself is

interstate in nature, or computers used in interstate and foreign commerce. It was amended in

1986, 1994, 1996, in 2001 by the USA PATRIOT

Act, and in 2008 by the Identity Theft Enforcement and Restitution Act. Section (b) of the act

punishes anyone who not just commits or

attempts to commit an offense under the Computer Fraud and Abuse Act but also those who conspire to do so.

Answer option B is incorrect. The Computer Security Act was passed by the United States Congress. It was passed to improve the security and privacy of sensitive information in Federal computer systems and to establish a minimum acceptable security practices for such systems. It requires the creation of computer security plans, and the appropriate training of system users or owners where the systems house sensitive information.

Answer option C is incorrect. The Gramm-Leach-Bliley Act (GLBA) is also known as the Financial Services Modernization Act of 1999. It is an act of the 106th United States Congress (1999-2001) signed into law by President Bill Clinton which repealed part of the Glass-Steagall Act of 1933, opening up the market among banking companies, securities companies and insurance companies.

The Gramm-Leach-Bliley Act allowed commercial banks, investment banks, securities firms, and insurance companies to consolidate. This law also provides regulations regarding the way financial institutions handle private information belongings to their clients.

Answer option D is incorrect. The Digital Millennium Copyright Act (DMCA) is a United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO). It criminalizes production and dissemination of technology, devices, or services intended to circumvent measures (commonly known as digital rights management or DRM) that control access to copyrighted works.

It also criminalizes the act of circumventing an access control, whether or not there is actual infringement of copyright itself. In addition, the DMCA heightens the penalties for copyright infringement on the Internet.

Question 9

Question Type: MultipleChoice

Which of the following individuals are part of the senior management and are responsible for authorization of individual systems, approving enterprise solutions, establishing security policies, providing funds, and maintaining an understanding of risks at all levels? Each correct answer represents a complete solution. Choose all that apply.

Options:

A- Chief Information Officer

B- AO Designated Representative

C- Senior Information Security Officer

D- User Representative

E- Authorizing Official

Answer:

A, B, C, E

Explanation:

Authorizing Official, AO Designated Representative (AODR), Chief Information Officer (CIO), and

Senior Information Security Officer (SISO) are part of the senior management. These individuals are responsible for the following:

Authorization of individual systems

Approving enterprise solutions

Establishing security policies

Providing funds

Maintaining an understanding of risk at all levels

Answer option D is incorrect. A User Representative is not a part of the senior management in the Authorization process.

Question 10

Question Type: **MultipleChoice**

FIPS 199 defines the three levels of potential impact on organizations: low, moderate, and high. Which of the following are the effects of loss of confidentiality, integrity, or availability in a high level potential impact?

Options:

A- The loss of confidentiality, integrity, or availability might cause severe degradation in or loss of mission capability to an extent.

B- The loss of confidentiality, integrity, or availability might result in major financial losses.

C- The loss of confidentiality, integrity, or availability might result in a major damage to organizational assets.

D- The loss of confidentiality, integrity, or availability might result in severe damages like life threatening injuries or loss of life.

Answer:

A, B, C, D

Explanation:

The following are the effects of loss of confidentiality, integrity, or availability in a high level

potential impact:

It might cause a severe degradation in or loss of mission capability to an extent.

It might result in a major damage to organizational assets.

It might result in a major financial loss.

It might result in severe harms such as serious life threatening injuries or loss of life.

Question 11

Question Type: MultipleChoice

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.

Options:

A- Type accreditation

B- Site accreditation

C- System accreditation

D- Secure accreditation

Answer:

A, B, C

Explanation:

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 option D is incorrect. No such type of NIACAP accreditation exists.