Free Questions for ISSEP by dumpssheet

Shared by Johnson on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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.

Options:

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 is the fourth phase of the security certification and accreditation process.

The Continuous Monitoring process consists of the following three main activities:

Configuration management and control Security control monitoring and impact analyses of changes

to the information system Status reporting and documentation The objective of these tasks is to

observe and evaluate the information system security controls during the system life cycle. These

tasks determine whether the changes that have occurred will negatively impact the system security.

Answer options E and D are incorrect. Security accreditation decision and security accreditation

documentation are the two tasks of the security accreditation phase.

Question 2

Question Type: **MultipleChoice**

You are working as a project manager in your organization. You are nearing the final stages of project execution and looking towards the final risk monitoring and controlling activities. For your project archives, which one of the following is an output of risk monitoring and control?

Options:

A- Quantitative risk analysis

B- Risk audits

C- Requested changes

D- Qualitative risk analysis

Answer:

C

Explanation:

Of all the choices presented, only requested changes is an output of the monitor and control risks

process. You might also have risk register

updates, recommended corrective and preventive actions, organizational process assets, and

updates to the project management plan.

Answer options D and A are incorrect. These are the plan risk management processes.

Answer option B is incorrect. Risk audit is a risk monitoring and control technique.

Question 3

Question Type: MultipleChoice

Which of the following are the major tasks of riskmanagement? Each correct answer represents acomplete solution. Choose two.

Options:

A- Riskidentification

B- Building Risk free systems

C- Assuring the integrity of organizational data

D- Risk control

Answer:

A, D

Explanation:

The following are the two major tasks of risk management:

1.Risk identification

2.Risk control

Risk identification is the task of examining and documenting the security posture of an organization's information technology and the risks it faces.

Risk control is the task of applying controls to reduce risks to an organization's data and information systems.

Answer options B and C are incorrect. Building risk free systems and assuring the integrity of organizational data are the tasks related to the implementation of security measures.

Question 4

Question Type: **MultipleChoice**

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

Options:

A- Type III cryptography

B- Type III (E) cryptography

C- Type II cryptography

D- Type I cryptography

Answer:

D

Explanation:

The types ofcryptography defined by FIPS 185 are as follows:

Type I cryptography: It describes a cryptographic algorithm or a tool accepted bythe NationalSecurity Agency for protecting classifiedinformation.

Type II cryptography: It describes a cryptographic algorithm or a tool accepted by theNationalSecurity Agency for protectingsensitive, unclassifiedinformation in the systems as stated in Section 2315 ofTitle 10, United StatesCode, or Section3502(2) ofTitle44, United States Code.

Type III cryptography: It describes a cryptographic algorithm or a tool accepted as a FederalInformation Processing Standard.

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

Question 5

Question Type: MultipleChoice

Which of the following types of CNSS issuances establishes criteria, and assigns responsibilities?

Options:

A- Advisory memoranda

B- Directives

C- Instructions

D- Policies

Answer:

D

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 howto implement the policy or prescribes the manner of a policy (NSTISSI).

Advisory memoranda: It providesguidance on policy and may cover avariety of topics involvinginformation assurance,

telecommunications security, and network security (NSTISSAM).

Question 6

Question Type: MultipleChoice

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.

Options:

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:

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.