Vendor:ISC

Exam Code:ISSEP

Exam Name:ISSEP Information Systems Security Engineering Professional

Version: Demo

QUESTION 1

What are the subordinate tasks of the Initiate and Plan IA CandA phase of the DIACAP process Each correct answer represents a complete solution. Choose all that apply.

A. Develop DIACAP strategy.

B. Initiate IA implementation plan.

C. Conduct validation activity.

D. Assemble DIACAP team.

E. Register system with DoD Component IA Program.

F. Assign IA controls.

Correct Answer: ABDEF

QUESTION 2

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

A. Data security requirement

B. Network connection rule

C. Applicable instruction or directive

D. Security concept of operation

Correct Answer: A

QUESTION 3

A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. What are the different types of policies Each correct answer represents a complete solution. Choose all that apply.

A. Regulatory

B. Advisory

C. Systematic

D. Informative

Correct Answer: ABD

QUESTION 4

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

A. DoD 8500.2 Information Assurance Implementation

B. DoD 8510.1-M DITSCAP

C. DoDI 5200.40

D. DoD 8500.1 Information Assurance (IA)

Correct Answer: D

QUESTION 5

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

Correct Answer: BD

QUESTION 6

Your project team has identified a project risk that must be responded to. The risk has been recorded in the risk register and the project team has been discussing potential risk responses for the risk event. The event is not likely to happen for several months but the probability of the event is high. Which one of the following is a valid response to the identified risk event

A. Earned value management

B. Risk audit

C. Corrective action

D. Technical performance measurement

Correct Answer: C

QUESTION 7

Which of the following federal laws is designed to protect computer data from theft

A. Federal Information Security Management Act (FISMA)

B. Computer Fraud and Abuse Act (CFAA)

C. Government Information Security Reform Act (GISRA)

D. Computer Security Act

Correct Answer: B

QUESTION 8

Which of the following is the acronym of RTM

A. Resource tracking method

B. Requirements Testing Matrix

C. Requirements Traceability Matrix

D. Resource timing method

Correct Answer: C

QUESTION 9

There are seven risk responses for any project. Which one of the following is a valid risk response for a negative risk event

A. Acceptance

B. Enhance

C. Share

D. Exploit

Correct Answer: A

QUESTION 10

Which of the following is a 1996 United States federal law, designed to improve the way the federal government acquires, uses, and disposes information technology

A. Lanham Act

B. Clinger-Cohen Act

C. Computer Misuse Act

D. Paperwork Reduction Act

Correct Answer: B

QUESTION 11

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

A. NSTISSP No. 7

B. NSTISSP No. 11

C. NSTISSP No. 6

D. NSTISSP No. 101

Correct Answer: C

QUESTION 12

An Authorizing Official plays the role of an approver. What are the responsibilities of an Authorizing Official Each correct answer represents a complete solution. Choose all that apply.

A. Ascertaining the security posture of the organization\\'s information system

B. Reviewing security status reports and critical security documents

C. Determining the requirement of reauthorization and reauthorizing information systems when required

D. Establishing and implementing the organization\\'s continuous monitoring program

Correct Answer: ABC