ISC

Exam CAP

CAP – Certified Authorization Professional

Version: 6.0

[Total Questions: 395]

Topic 1, Volume A

Question No : 1 - (Topic 1)

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

A. Senior Agency Information Security Officer
B. Authorizing Official
C. Common Control Provider
D. Chief Information Officer

Answer: C

Question No : 2 - (Topic 1)

The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise. What are the responsibilities of a Chief Information Officer?

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

A. Preserving high-level communications and working group relationships in an organization
B. Facilitating the sharing of security risk-related information among authorizing officials
C. Establishing effective continuous monitoring program for the organization
D. Proposing the information technology needed by an enterprise to achieve its goals and then working within a budget to implement the plan

Answer: A,C,D

Question No : 3 - (Topic 1)

The Information System Security Officer (ISSO) and Information System Security Engineer (ISSE) play the role of a supporter and advisor, respectively. Which of the following statements are true about ISSO and ISSE?

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

A. An ISSE provides advice on the impacts of system changes.
B. An ISSE manages the security of the information system that is slated for Certification & Accreditation (C&A).
C. An ISSO manages the security of the information system that is slated for Certification & Accreditation (C&A).
D. An ISSO takes part in the development activities that are required to implement system changes.
E. An ISSE provides advice on the continuous monitoring of the information system.

Answer: A,C,E

Question No : 4 - (Topic 1)

Which of the following professionals is responsible for starting the Certification & Accreditation (C&A) process?

A. Information system owner
B. Authorizing Official
C. Chief Risk Officer (CRO)
D. Chief Information Officer (CIO)

Answer: A

Question No : 5 - (Topic 1)

Which of the following assessment methodologies defines a six-step technical security evaluation?

A. FITSAF
B. FIPS 102
C. OCTAVE
D. DITSCAP

Answer: B

Question No : 6 - (Topic 1)

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. What phases are identified by DIACAP?

Each correct answer represents acomplete solution. Choose all that apply.

A. Accreditation
B. Identification
C. System Definition
D. Verification
E. Validation
F. Re-Accreditation

Answer: C,D,E,F

Question No : 7 - (Topic 1)

Mark works as a Network Administrator for NetTech Inc. He wants users to access only those resources that are required for them. Which of the following access control models will he use?

A. Mandatory Access Control
B. Role-Based Access Control
C. Discretionary Access Control
D. Policy Access Control

Answer: B

Question No : 8 - (Topic 1)

Which of the following refers to an information security document that is used in the United States Department of Defense (DoD) to describe and accredit networks and systems?

A. FITSAF
B. FIPS
C. TCSEC
D. SSAA

Answer: D

Question No : 9 - (Topic 1)

James work as an IT systems personnel in SoftTech Inc. He performs the following tasks:

Runs regular backups and routine tests of the validity of the backup data.

Performs data restoration from the backups whenever required.

Maintains the retained records in accordance with the established information classification policy.

What is the role played by James in the organization?

A. Manager
B. Owner
C. Custodian
D. User

Answer: C

Question No : 10 - (Topic 1)

FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls have been implemented?

A. Level 4
B. Level 1
C. Level 3
D. Level 5
E. Level 2

Answer: C

Question No : 11 - (Topic 1)

Certification and Accreditation (C&A or CnA) is a process for implementing information security.

Which of the following is the correct order of C&A phases in a DITSCAP assessment?

A. Definition, Validation, Verification, and Post Accreditation
B. Verification, Definition, Validation, and Post Accreditation
C. Verification, Validation, Definition, and Post Accreditation
D. Definition, Verification, Validation, and Post Accreditation

Answer: D

Question No : 12 - (Topic 1)

System Authorization is the risk management process. System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. What are the different phases of System Authorization Plan?

Each correct answer represents a part of the solution. Choose all that apply.

A. Post-Authorization
B. Pre-certification
C. Post-certification
D. Certification
E. Authorization

Answer: A,B,D,E

Question No : 13 - (Topic 1)

Certification and Accreditation (C&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. Which of the following statements are true about Certification and Accreditation?

Each correct answer represents a complete solution. Choose two.

A. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system.
B. Accreditation is a comprehensive assessment of the management, operational, and technical security controls in an information system.
C. Certification is the official management decision given by a senior agency official to authorize operation of an information system.
D. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system.

Answer: A,D

Question No : 14 - (Topic 1)

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 apart of the solution. Choose all that apply.

A. NIST
B. FIPS
C. FISMA
D. Office of Management and Budget (OMB)

Answer: C,D

Question No : 15 - (Topic 1)

The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum standard processfor 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.

A. Secure accreditation
B. Type accreditation
C. System accreditation
D. Site accreditation

Answer: B,C,D

Question No : 16 - (Topic 1)

According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information

Assurance (IA) areas, and the controls are referred to as IA controls. Which of the following are among the eight areas of IA defined by DoD?

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

A. VI Vulnerability and Incident Management
B. DC Security Design & Configuration
C. EC Enclave and Computing Environment
D. Information systems acquisition, development, and maintenance

Answer: A,B,C

Question No : 17 - (Topic 1)

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. What phases are identified by DIACAP?

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

A. Validation
B. Re-Accreditation
C. Verification
D. System Definition
E. Identification
F. Accreditation

Answer: A,B,C,D

Question No : 18 - (Topic 1)

Which of the following is a subset discipline of Corporate Governance focused on information security systems and their performance and risk management?

A. Lanham Act
B. ISG
C. Clinger-Cohen Act
D. Computer Misuse Act

Answer: B

Question No : 19 - (Topic 1)

Ben is the project manager of the YHT Project for his company. Alice, one of his team members, is confused about when project risks will happen in the project. Which one of the following statements is the most accurate about when project risk happens?

A. Project risk can happen at any moment.
B. Project risk is uncertain, so no one can predict when the event will happen.
C. Project risk happens throughout the project execution.
D. Project riskis always in the future.

Answer: D

Question No : 20 - (Topic 1)

You are the project manager of the NKJ Project for your company. The project's success or failure will have a significant impact on your organization's profitability for the coming year. Management has asked you to identify the risk events and communicate the event's probability and impact as early as possible in the project. Management wants to avoid risk events and needs to analyze the cost-benefits of each risk event in this project. What term is assigned to the low-level of stakeholder tolerance in this project?

A. Risk avoidance
B. Mitigation-ready project management
C. Risk utility function
D. Risk-reward mentality

Answer: C

Question No : 21 - (Topic 1)

Where can a project manager find risk-rating rules?

A. Risk probability and impact matrix
B. Organizational process assets
C. Enterprise environmental factors

D. Risk management plan

Answer: B

Question No : 22 - (Topic 1)

There are five inputs to the quantitative risk analysis process. Which one of the following isNOTan input to the perform quantitative risk analysis process?

A. Risk register
B. Cost management plan
C. Risk management plan
D. Enterprise environmental factors

Answer: D

Question No : 23 - (Topic 1)

Your project has several risks that may cause serious financial impact should they happen.You have studied the risk events and made some potential risk responses for the risk events but management wants you to do more. They'd like for you to create some type of a chart that identified the risk probability and impact with a financialamount for each risk event. What is the likely outcome of creating this type of chart?

A. Risk response plan
B. Quantitative analysis
C. Risk response
D. Contingency reserve

Answer: D

Question No : 24 - (Topic 1)

Which of the following professionals is responsible forstarting the Certification & Accreditation

(C&A) process?