ISC2

CAP Exam

ISC2 CAP Certified Authorization Professional Exam

Question: 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: 2

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: 3

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: 4

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: 5

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: 6

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

Answer: C,D,E,F

Question: 7

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: 8

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: 9

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: 10

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: 11

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: 12

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: 13

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: 14

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.

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

Answer: C,D

Question: 15

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.

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

Answer: B,C,D