



ISC2

Exam Questions CISSP-ISSEP

Information Systems Security Engineering Professional

NEW QUESTION 1

Which of the following approaches can be used to build a security program Each correct answer represents a complete solution. Choose all that apply.

- A. Right-Up Approach
- B. Left-Up Approach
- C. Bottom-Up Approach
- D. Top-Down Approach

Answer: CD

NEW QUESTION 2

Fill in the blank with the appropriate phrase. provides instructions and directions for completing the Systems Security Authorization Agreement (SSAA).

- A. DoDI 5200.40

Answer: A

NEW QUESTION 3

Which of the following phases of DITSCAP includes the activities that are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle

- A. Phase 1, Definition
- B. Phase 3, Validation
- C. Phase 4, Post Accreditation Phase
- D. Phase 2, Verification

Answer: C

NEW QUESTION 4

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

Answer: ABDE

NEW QUESTION 5

Which of the following documents contains the threats to the information management, and the security services and controls required to counter those threats

- A. System Security Context
- B. Information Protection Policy (IPP)
- C. CONOPS
- D. IMM

Answer: B

NEW QUESTION 6

Which of the following documents were developed by NIST for conducting Certification & Accreditation (C&A) Each correct answer represents a complete solution. Choose all that apply.

- A. NIST Special Publication 800-59
- B. NIST Special Publication 800-60
- C. NIST Special Publication 800-37A
- D. NIST Special Publication 800-37
- E. NIST Special Publication 800-53
- F. NIST Special Publication 800-53A

Answer: ABDEF

NEW QUESTION 7

Which of the following types of cryptography defined by FIPS 185 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

- A. Type I cryptography
- B. Type II cryptography
- C. Type III (E) cryptography
- D. Type III cryptography

Answer: B

NEW QUESTION 8

Which of the following is a standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system

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

Answer: B

NEW QUESTION 9

TQM recognizes that quality of all the processes within an organization contribute to the quality of the product. Which of the following are the most important activities in the Total Quality Management Each correct answer represents a complete solution. Choose all that apply.

- A. Quality renewal
- B. Maintenance of quality
- C. Quality costs
- D. Quality improvements

Answer: ABD

NEW QUESTION 10

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

- A. Advisory memoranda
- B. Directives
- C. Instructions
- D. Policies

Answer: D

NEW QUESTION 10

Which of the following organizations is a USG initiative designed to meet the security testing, evaluation, and assessment needs of both information technology (IT) producers and consumers

- A. NSA
- B. NIST
- C. CNSS
- D. NIAP

Answer: D

NEW QUESTION 15

The DoD 8500 policy series represents the Department's information assurance strategy. Which of the following objectives are defined by the DoD 8500 series Each correct answer represents a complete solution. Choose all that apply.

- A. Providing IA Certification and Accreditation
- B. Providing command and control and situational awareness
- C. Defending systems
- D. Protecting information

Answer: BCD

NEW QUESTION 16

Which of the following security controls is a set of layered security services that address communications and data security problems in the emerging Internet and intranet application space

- A. Internet Protocol Security (IPSec)
- B. Common data security architecture (CDSA)
- C. File encryptors
- D. Application program interface (API)

Answer: B

NEW QUESTION 20

Fill in the blank with the appropriate phrase. The is the risk that remains after the implementation of new or enhanced controls.

- A. residual risk

Answer: A

NEW QUESTION 24

Fill in the blank with an appropriate section name. is a section of the SEMP template, which specifies the methods and reasoning planned to build the requisite trade-offs between functionality, performance, cost, and risk.

A. System Analysis

Answer: A

NEW QUESTION 27

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 are tested and reviewed

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

Answer: A

NEW QUESTION 32

Which of the following persons in an organization is responsible for rejecting or accepting the residual risk for a system

- A. System Owner
- B. Information Systems Security Officer (ISSO)
- C. Designated Approving Authority (DAA)
- D. Chief Information Security Officer (CISO)

Answer: C

NEW QUESTION 37

You work as a systems engineer for BlueWell Inc. You are working on translating system requirements into detailed function criteria. Which of the following diagrams will help you to show all of the function requirements and their groupings in one diagram

- A. Activity diagram
- B. Functional flow block diagram (FFBD)
- C. Functional hierarchy diagram
- D. Timeline analysis diagram

Answer: C

NEW QUESTION 42

Which of the following areas of information system, as separated by Information Assurance Framework, is a collection of local computing devices, regardless of physical location, that are interconnected via local area networks (LANs) and governed by a single security policy

- A. Networks and Infrastructures
- B. Supporting Infrastructures
- C. Enclave Boundaries
- D. Local Computing Environments

Answer: C

NEW QUESTION 44

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

- A. Type III cryptography
- B. Type III (E) cryptography
- C. Type II cryptography
- D. Type I cryptography

Answer: D

NEW QUESTION 49

What are the subordinate tasks of the Implement and Validate Assigned IA Control phase in the DIACAP process Each correct answer represents a complete solution. Choose all that apply.

- A. Conduct activities related to the disposition of the system data and objects.
- B. Combine validation results in DIACAP scorecard.
- C. Conduct validation activities.
- D. Execute and update IA implementation plan.

Answer: BCD

NEW QUESTION 54

For interactive and self-paced preparation of exam ISSEP, try our practice exams. Practice exams also include self assessment and reporting features! Fill in the blank with an appropriate word. has the goal to securely interconnect people and systems independent of time or location.

- A. Netcentric

Answer: A

NEW QUESTION 58

What are the responsibilities of a system owner Each correct answer represents a complete solution. Choose all that apply.

- A. Integrates security considerations into application and system purchasing decisions and development projects.
- B. Ensures that the necessary security controls are in place.
- C. Ensures that adequate security is being provided by the necessary controls, password management, remote access controls, operating system configurations, and so on.
- D. Ensures that the systems are properly assessed for vulnerabilities and must report any to the incident response team and data owner.

Answer: ACD

NEW QUESTION 63

Which of the following federal agencies has the objective to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life

- A. National Institute of Standards and Technology (NIST)
- B. National Security Agency (NSA)
- C. Committee on National Security Systems (CNSS)
- D. United States Congress

Answer: A

NEW QUESTION 66

Which of the following processes culminates in an agreement between key players that a system in its current configuration and operation provides adequate protection controls

- A. Certification and accreditation (C&A)
- B. Risk Management
- C. Information systems security engineering (ISSE)
- D. Information Assurance (IA)

Answer: A

NEW QUESTION 69

Which of the following certification levels requires the completion of the minimum security checklist, and the system user or an independent certifier can complete the checklist

- A. CL 2
- B. CL 3
- C. CL 1
- D. CL 4

Answer: C

NEW QUESTION 72

Which of the following is NOT used in the practice of Information Assurance (IA) to define assurance requirements

- A. Classic information security model
- B. Five Pillars model
- C. Communications Management Plan
- D. Parkerian Hexad

Answer: C

NEW QUESTION 76

Fill in the blank with an appropriate phrase. seeks to improve the quality of process outputs by identifying and removing the causes of defects and variability in manufacturing and business processes.

- A. Six Sigma

Answer: A

NEW QUESTION 79

Numerous information security standards promote good security practices and define frameworks or systems to structure the analysis and design for managing information security controls. Which of the following are the international information security standards Each correct answer represents a complete solution. Choose all that apply.

- A. Organization of information security
- B. Human resources security
- C. Risk assessment and treatment
- D. AU audit and accountability

Answer: ABC

NEW QUESTION 81

Which of the following types of CNSS issuances describes how to implement the policy or prescribes the manner of a policy

- A. Advisory memoranda
- B. Instructions
- C. Policies
- D. Directives

Answer: B

NEW QUESTION 85

Which of the following DITSCAP phases validates that the preceding work has produced an IS that operates in a specified computing environment

- A. Phase 4
- B. Phase 2
- C. Phase 1
- D. Phase 3

Answer: D

NEW QUESTION 86

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 missionbusiness needs. Which of the following processes will John use to achieve the task

- A. Modes of operation
- B. Performance requirement
- C. Functional requirement
- D. Technical performance measures

Answer: C

NEW QUESTION 87

Which of the following individuals informs all C&A participants about life cycle actions, security requirements, and documented user needs

- A. User representative
- B. DAA
- C. Certification Agent
- D. IS program manager

Answer: D

NEW QUESTION 89

Which of the following processes illustrate the study of a technical nature of interest to focused audience, and consist of interim or final reports on work made by NIST for external sponsors, including government and non-government sponsors

- A. Federal Information Processing Standards (FIPS)
- B. Special Publication (SP)
- C. NISTIRs (Internal Reports)
- D. DIACAP

Answer: C

NEW QUESTION 90

Which of the following individuals is responsible for monitoring the information system environment for factors that can negatively impact the security of the system and its accreditation

- A. Chief Information Officer
- B. Chief Information Security Officer
- C. Chief Risk Officer
- D. Information System Owner

Answer: D

NEW QUESTION 92

Which of the following protocols is used to establish a secure terminal to a remote network device

- A. WEP
- B. SMTP
- C. SSH
- D. IPSec

Answer: C

NEW QUESTION 94

Which of the following configuration management system processes defines which items will be configuration managed, how they are to be identified, and how they are to be documented

- A. Configuration verification and audit
- B. Configuration control
- C. Configuration status accounting
- D. Configuration identification

Answer: D

NEW QUESTION 95

Which of the following agencies provides command and control capabilities and enterprise infrastructure to continuously operate and assure a global net-centric enterprise in direct support to joint warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations

- A. DARPA
- B. DTIC
- C. DISA
- D. DIAP

Answer: C

NEW QUESTION 99

DoD 8500.2 establishes IA controls for information systems according to the Mission Assurance Categories (MAC) and confidentiality levels. Which of the following MAC levels requires basic integrity and availability

- A. MAC I
- B. MAC II
- C. MAC IV
- D. MAC III

Answer: D

NEW QUESTION 100

Which of the following DITSCAP C&A phases takes place between the signing of the initial version of the SSAA and the formal accreditation of the system

- A. Phase 3
- B. Phase 2
- C. Phase 4
- D. Phase 1

Answer: B

NEW QUESTION 101

Which of the following DITSCAPNIACAP model phases is used to show the required evidence to support the DAA in accreditation process and conclude in an Approval To Operate (ATO)

- A. Verification
- B. Validation
- C. Post accreditation
- D. Definition

Answer: B

NEW QUESTION 102

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

Answer: A

NEW QUESTION 105

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

Answer: ABC

NEW QUESTION 109

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)

Answer: D

NEW QUESTION 111

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

- A. Computer Fraud and Abuse Act
- B. Computer Security Act
- C. Gramm-Leach-Bliley Act
- D. Digital Millennium Copyright Act

Answer: A

NEW QUESTION 112

Numerous information security standards promote good security practices and define frameworks or systems to structure the analysis and design for managing information security controls. Which of the following are the U.S. Federal Government information security standards Each correct answer represents a complete solution. Choose all that apply.

- A. CA Certification, Accreditation, and Security Assessments
- B. Information systems acquisition, development, and maintenance
- C. IR Incident Response
- D. SA System and Services Acquisition

Answer: ACD

NEW QUESTION 116

Which of the following is used to indicate that the software has met a defined quality level and is ready for mass distribution either by electronic means or by physical media

- A. ATM
- B. RTM
- C. CRO
- D. DAA

Answer: B

NEW QUESTION 117

Which of the following categories of system specification describes the technical, performance, operational, maintenance, and support characteristics for the entire system

- A. Process specification
- B. Product specification
- C. Development specification
- D. System specification

Answer: D

NEW QUESTION 118

The functional analysis process is used for translating system requirements into detailed function criteria. Which of the following are the elements of functional analysis process Each correct answer represents a complete solution. Choose all that apply.

- A. Model possible overall system behaviors that are needed to achieve the system requirements.
- B. Develop concepts and alternatives that are not technology or component bound.
- C. Decompose functional requirements into discrete tasks or activities, the focus is still on technology not functions or components.
- D. Use a top-down with some bottom-up approach verification.

Answer: ABD

NEW QUESTION 122

Which of the following processes describes the elements such as quantity, quality, coverage, timelines, and availability, and categorizes the different functions that the system will need to perform in order to gather the documented missionbusiness needs

- A. Functional requirements
- B. Operational scenarios
- C. Human factors
- D. Performance requirements

Answer: A

NEW QUESTION 123

What NIACAP certification levels are recommended by the certifier Each correct answer represents a complete solution. Choose all that apply.

- A. Basic System Review
- B. Basic Security Review
- C. Maximum Analysis
- D. Comprehensive Analysis
- E. Detailed Analysis
- F. Minimum Analysis

Answer: BDEF

NEW QUESTION 124

Which of the following types of firewalls increases the security of data packets by remembering the state of connection at the network and the session layers as they pass through the filter

- A. Stateless packet filter firewall
- B. PIX firewall
- C. Stateful packet filter firewall
- D. Virtual firewall

Answer: C

NEW QUESTION 125

According to which of the following DoD policies, the implementation of DITSCAP is mandatory for all the systems that process both DoD classified and unclassified information?

- A. DoD 8500.2
- B. DoDI 5200.40
- C. DoD 8510.1-M DITSCAP
- D. DoD 8500.1 (IAW)

Answer: D

NEW QUESTION 126

Which of the following protocols is built in the Web server and browser to encrypt data traveling over the Internet

- A. UDP
- B. SSL
- C. IPSec
- D. HTTP

Answer: B

NEW QUESTION 129

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

Answer: ABD

NEW QUESTION 134

Which of the following principles are defined by the IATF model Each correct answer represents a complete solution. Choose all that apply.

- A. The degree to which the security of the system, as it is defined, designed, and implemented, meets the security needs.
- B. The problem space is defined by the customer's mission or business needs.
- C. The systems engineer and information systems security engineer define the solution space, which is driven by the problem space.
- D. Always keep the problem and solution spaces separate.

Answer: BCD

NEW QUESTION 136

Which of the following techniques are used after a security breach and are intended to limit the extent of any damage caused by the incident

- A. Corrective controls
- B. Safeguards
- C. Detective controls
- D. Preventive controls

Answer: A

NEW QUESTION 141

Which of the of following departments protects and supports DoD information, information systems, and information networks that are critical to the department and the armed forces during the day-to-day operations, and in the time of crisis

- A. DIAP
- B. DARPA
- C. DTIC
- D. DISA

Answer: A

NEW QUESTION 142

Della works as a systems engineer for BlueWell Inc. She wants to convert system requirements into a comprehensive function standard, and break the higher-level functions into lower-level functions. Which of the following processes will Della use to accomplish the task

- A. Risk analysis
- B. Functional allocation
- C. Functional analysis
- D. Functional baseline

Answer: C

NEW QUESTION 147

Which of the following are the subtasks of the Define Life-Cycle Process Concepts task Each correct answer represents a complete solution. Choose all that apply.

- A. Training
- B. Personnel
- C. Control
- D. Manpower

Answer: ABD

NEW QUESTION 148

Which of the following Registration Tasks notifies the DAA, Certifier, and User Representative that the system requires C&A Support

- A. Registration Task 4
- B. Registration Task 1
- C. Registration Task 3
- D. Registration Task 2

Answer: D

NEW QUESTION 150

Which of the following DoD directives defines DITSCAP as the standard C&A process for the Department of Defense

- A. DoD 5200.22-M
- B. DoD 8910.1
- C. DoD 5200.40
- D. DoD 8000.1

Answer: C

NEW QUESTION 155

Which of the following is the application of statistical methods to the monitoring and control of a process to ensure that it operates at its full potential to produce conforming product

- A. Information Assurance (IA)
- B. Statistical process control (SPC)
- C. Information Protection Policy (IPP)
- D. Information management model (IMM)

Answer: B

NEW QUESTION 157

Which of the following organizations incorporates building secure audio and video communications equipment, making tamper protection products, and providing trusted microelectronics solutions

- A. DTIC
- B. NSA IAD
- C. DIAP
- D. DARPA

Answer: B

NEW QUESTION 161

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.

- 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: ABC

NEW QUESTION 162

Fill in the blank with an appropriate phrase. A is defined as any activity that has an effect on defining, designing, building, or executing a task, requirement, or procedure.

- A. technical effort

Answer: A

NEW QUESTION 165

Which of the following responsibilities are executed by the federal program manager

- A. Ensure justification of expenditures and investment in systems engineering activities.
- B. Coordinate activities to obtain funding.
- C. Review project deliverables.
- D. Review and approve project plans.

Answer: ABD

NEW QUESTION 169

Which of the following DoD directives is referred to as the Defense Automation Resources Management Manual

- A. DoD 8910.1
- B. DoD 7950.1-M
- C. DoD 5200.22-M
- D. DoD 5200.1-R
- E. DoDD 8000.1

Answer: B

NEW QUESTION 170

Which of the following security controls works as the totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy

- A. Trusted computing base (TCB)
- B. Common data security architecture (CDSA)
- C. Internet Protocol Security (IPSec)
- D. Application program interface (API)

Answer: A

NEW QUESTION 172

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

- 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: ABCD

NEW QUESTION 176

Your project is an agricultural-based project that deals with plant irrigation systems. You have discovered a byproduct in your project that your organization could use to make a profit. If your organization seizes this opportunity it would be an example of what risk response

- A. Enhancing
- B. Positive
- C. Opportunistic
- D. Exploiting

Answer: D

NEW QUESTION 179

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

CISSP-ISSEP Practice Exam Features:

- * CISSP-ISSEP Questions and Answers Updated Frequently
- * CISSP-ISSEP Practice Questions Verified by Expert Senior Certified Staff
- * CISSP-ISSEP Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CISSP-ISSEP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CISSP-ISSEP Practice Test Here](#)