



ISC2

Exam Questions CISSP-ISSEP

Information Systems Security Engineering Professional

NEW QUESTION 1

Which of the following DoD policies provides assistance on how to implement policy, assign responsibilities, and prescribe procedures for applying integrated, layered protection of the DoD information systems and networks

- A. DoD 8500.1 Information Assurance (IA)
- B. DoDI 5200.40
- C. DoD 8510.1-M DITSCAP
- D. DoD 8500.2 Information Assurance Implementation

Answer: D

NEW QUESTION 2

Which of the following are the functional analysis and allocation tools Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ACD

NEW QUESTION 3

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 4

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 5

Which of the following acts is used to recognize the importance of information security to the economic and national security interests of the United States

- A. Lanham Act
- B. FISMA
- C. Computer Fraud and Abuse Act
- D. Computer Misuse Act

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 NIST documents describes that minimizing negative impact on an organization and a need for sound basis in decision making are the fundamental reasons organizations implement a risk management process for their IT systems

- A. NIST SP 800-37
- B. NIST SP 800-30
- C. NIST SP 800-53
- D. NIST SP 800-60

Answer: B

NEW QUESTION 8

Which of the following cooperative programs carried out by NIST conducts research to advance the nation's technology infrastructure

- A. Manufacturing Extension Partnership
- B. NIST Laboratories
- C. Baldrige National Quality Program
- D. Advanced Technology Program

Answer: B

NEW QUESTION 9

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 financial amount 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

NEW QUESTION 10

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 10

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 12

You work as a security engineer for BlueWell Inc. Which of the following documents will you use as a guide for the security certification and accreditation of Federal Information Systems

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

Answer: B

NEW QUESTION 14

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 17

You work as a security engineer for BlueWell Inc. According to you, which of the following statements determines the main focus of the ISSE process

- A. Design information systems that will meet the certification and accreditation documentation.
- B. Identify the information protection needs.
- C. Ensure information systems are designed and developed with functional relevance.
- D. Instruct systems engineers on availability, integrity, and confidentiality.

Answer: B

NEW QUESTION 20

Which of the following is a temporary approval to operate based on an assessment of the implementation status of the assigned IA Controls

- A. IATO
- B. DATO
- C. ATO
- D. IATT

Answer: A

NEW QUESTION 23

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 28

In which of the following phases of the interconnection life cycle as defined by NIST SP 800-47, do the organizations build and execute a plan for establishing the interconnection, including executing or configuring appropriate security controls

- A. Establishing the interconnection
- B. Planning the interconnection
- C. Disconnecting the interconnection
- D. Maintaining the interconnection

Answer: A

NEW QUESTION 33

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 37

Which of the following federal laws are related to hacking activities Each correct answer represents a complete solution. Choose three.

- A. 18 U.S.
- B. 1030
- C. 18 U.S.
- D. 1029
- E. 18 U.S.
- F. 2510
- G. 18 U.S.
- H. 1028

Answer: ABC

NEW QUESTION 40

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

Answer: A

NEW QUESTION 42

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

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

Answer:

B

NEW QUESTION 47

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 49

Which of the following tasks prepares the technical management plan in planning the technical effort

- A. Task 10
- B. Task 9
- C. Task 7
- D. Task 8

Answer: B

NEW QUESTION 52

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 54

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 57

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 62

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 63

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 65

Which of the following Security Control Assessment Tasks evaluates the operational, technical, and the management security controls of the information system using the techniques and measures selected or developed

- A. Security Control Assessment Task 3
- B. Security Control Assessment Task 1
- C. Security Control Assessment Task 4
- D. Security Control Assessment Task 2

Answer: A

NEW QUESTION 67

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 69

In which of the following DIACAP phases is residual risk analyzed

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

Answer: E

NEW QUESTION 74

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 77

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 82

Which of the following statements is true about residual risks

- A. It can be considered as an indicator of threats coupled with vulnerability.
- B. It is a weakness or lack of safeguard that can be exploited by a threat.
- C. It is the probabilistic risk after implementing all security measures.
- D. It is the probabilistic risk before implementing all security measures.

Answer: C

NEW QUESTION 85

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 88

Which of the following individuals are part of the senior management and are responsible for authorization of individual systems, approving enterprise solutions, establishing security policies, providing funds, and maintaining an understanding of risks at all levels Each correct answer represents a complete solution. Choose all that apply.

- A. Chief Information Officer
- B. AO Designated Representative
- C. Senior Information Security Officer
- D. User Representative
- E. Authorizing Official

Answer: ABCE

NEW QUESTION 93

Which of the following CNSS policies describes the national policy on use of cryptomaterial by activities operating in high risk environments

- A. CNSSP N
- B. 14
- C. NCSC N
- D. 5
- E. NSTISSP N
- F. 6
- G. NSTISSP N
- H. 7

Answer: B

NEW QUESTION 96

Which of the following types of CNSS issuances establishes or describes policy and programs, provides authority, or assigns responsibilities

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

Answer: B

NEW QUESTION 101

Which of the following memorandums reminds the Federal agencies that it is required by law and policy to establish clear privacy policies for Web activities and to comply with those policies

- A. OMB M-01-08
- B. OMB M-03-19
- C. OMB M-00-07
- D. OMB M-00-13

Answer: D

NEW QUESTION 103

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

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

Answer: C

NEW QUESTION 105

You work as a systems engineer for BlueWell Inc. You want to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. Which of the following processes will you use to accomplish the task

- A. Information Assurance (IA)
- B. Risk Management
- C. Risk Analysis
- D. Information Systems Security Engineering (ISSE)

Answer: A

NEW QUESTION 110

In 2003, NIST developed a new Certification & Accreditation (C&A) guideline known as FIPS 199. What levels of potential impact are defined by FIPS 199 Each correct answer represents a complete solution. Choose all that apply.

- A. High
- B. Medium
- C. Low

D. Moderate

Answer: ABC

NEW QUESTION 114

Which of the following agencies serves the DoD community as the largest central resource for DoD and government-funded scientific, technical, engineering, and business related information available today

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

Answer: C

NEW QUESTION 115

Which of the following individuals is an upper-level manager who has the power and capability to evaluate the mission, business case, and budgetary needs of the system while also considering the security risks

- A. User Representative
- B. Program Manager
- C. Certifier
- D. DAA

Answer: D

NEW QUESTION 117

You work as a system engineer for BlueWell Inc. Which of the following documents will help you to describe the detailed plans, procedures, and schedules to guide the transition process

- A. Configuration management plan
- B. Transition plan
- C. Systems engineering management plan (SEMP)
- D. Acquisition plan

Answer: B

NEW QUESTION 121

Fill in the blank with an appropriate phrase. The process is used for allocating performance and designing the requirements to each function.

- A. functional allocation

Answer: A

NEW QUESTION 123

Lisa is the project manager of the SQL project for her company. She has completed the risk response planning with her project team and is now ready to update the risk register to reflect the risk response. Which of the following statements best describes the level of detail Lisa should include with the risk responses she has created

- A. The level of detail must define exactly the risk response for each identified risk.
- B. The level of detail is set of project risk governance.
- C. The level of detail is set by historical information.
- D. The level of detail should correspond with the priority ranking.

Answer: D

NEW QUESTION 126

Which of the following is a document, usually in the form of a table, that correlates any two baseline documents that require a many-to-many relationship to determine the completeness of the relationship

- A. FIPS 200
- B. NIST SP 800-50
- C. Traceability matrix
- D. FIPS 199

Answer: C

NEW QUESTION 127

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. Which of the following participants are required in a NIACAP security assessment Each correct answer represents a part of the solution. Choose all that apply.

- A. Information Assurance Manager
- B. Designated Approving Authority
- C. Certification agent

- D. IS program manager
- E. User representative

Answer: BCDE

NEW QUESTION 132

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 137

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 142

Della works as a security engineer for BlueWell Inc. She wants to establish configuration management and control procedures that will document proposed or actual changes to the information system. Which of the following phases of NIST SP 800-37 C&A methodology will define the above task

- A. Security Certification
- B. Security Accreditation
- C. Initiation
- D. Continuous Monitoring

Answer: D

NEW QUESTION 143

Which of the following types of cryptography defined by FIPS 185 describes a cryptographic algorithm or a tool accepted as a Federal Information Processing Standard

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

Answer: B

NEW QUESTION 148

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

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

Answer: C

NEW QUESTION 149

You work as a security manager for BlueWell Inc. You are going through the NIST SP 800-37 C&A methodology, which is based on four well defined phases. In which of the following phases of NIST SP 800-37 C&A methodology does the security categorization occur

- A. Continuous Monitoring
- B. Initiation
- C. Security Certification
- D. Security Accreditation

Answer: B

NEW QUESTION 152

You work as a Network Administrator for PassGuide Inc. You need to secure web services of your company in order to have secure transactions. Which of the following will you recommend for providing security

- A. HTTP
- B. VPN
- C. SMIME
- D. SSL

Answer: D

NEW QUESTION 157

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 161

Which of the following guidelines is recommended for engineering, protecting, managing, processing, and controlling national security and sensitive (although unclassified) information

- A. Federal Information Processing Standard (FIPS)
- B. Special Publication (SP)
- C. NISTIRs (Internal Reports)
- D. DIACAP by the United States Department of Defense (DoD)

Answer: B

NEW QUESTION 166

Which of the following DITSCAPNIACAP model phases is used to confirm that the evolving system development and integration complies with the agreements between role players documented in the first phase

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

Answer: A

NEW QUESTION 167

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 168

Which of the following rated systems of the Orange book has mandatory protection of the TCB

- A. C-rated
- B. B-rated
- C. D-rated
- D. A-rated

Answer: B

NEW QUESTION 169

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 173

Which of the following documents is described in the statement below It is developed along with all processes of the risk management. It contains the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning.

- A. Risk management plan

- B. Project charter
- C. Quality management plan
- D. Risk register

Answer: D

NEW QUESTION 176

Stella works as a system engineer for BlueWell Inc. She wants to identify the performance thresholds of each build. Which of the following tests will help Stella to achieve her task

- A. Regression test
- B. Reliability test
- C. Functional test
- D. Performance test

Answer: D

NEW QUESTION 180

You have been tasked with finding an encryption methodology that will encrypt most types of email attachments. The requirements are that your solution must use the RSA algorithm. Which of the following is your best choice

- A. PGP
- B. SMIME
- C. DES
- D. Blowfish

Answer: B

NEW QUESTION 182

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 183

Which of the following documents is defined as a source document, which is most useful for the ISSE when classifying the needed security functionality

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

Answer: A

NEW QUESTION 186

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 190

Which of the following acts is endorsed to provide a clear statement of the proscribed activity concerning computers to the law enforcement community, those who own and operate computers, and those tempted to commit crimes by unauthorized access to computers

- A. Computer Fraud and Abuse Act
- B. Government Information Security Reform Act (GISRA)
- C. Computer Security Act
- D. Federal Information Security Management Act (FISMA)

Answer: A

NEW QUESTION 192

Which of the following Security Control Assessment Tasks gathers the documentation and supporting materials essential for the assessment of the security controls in the information system

- A. Security Control Assessment Task 4

- B. Security Control Assessment Task 3
- C. Security Control Assessment Task 1
- D. Security Control Assessment Task 2

Answer: C

NEW QUESTION 193

The phase 3 of the Risk Management Framework (RMF) process is known as mitigation planning. Which of the following processes take place in phase 3 Each correct answer represents a complete solution. Choose all that apply.

- A. Agree on a strategy to mitigate risks.
- B. Evaluate mitigation progress and plan next assessment.
- C. Identify threats, vulnerabilities, and controls that will be evaluated.
- D. Document and implement a mitigation plan.

Answer: ABD

NEW QUESTION 198

Which of the following NIST Special Publication documents provides a guideline on questionnaires and checklists through which systems can be evaluated for compliance against specific control objectives

- A. NIST SP 800-53A
- B. NIST SP 800-37
- C. NIST SP 800-53
- D. NIST SP 800-26
- E. NIST SP 800-59
- F. NIST SP 800-60

Answer: D

NEW QUESTION 202

Which of the following tools demands involvement by upper executives, in order to integrate quality into the business system and avoid delegation of quality functions to junior administrators

- A. ISO 90012000
- B. Benchmarking
- C. SEI-CMM
- D. Six Sigma

Answer: A

NEW QUESTION 205

Diane is the project manager of the HGF Project. A risk that has been identified and analyzed in the project planning processes is now coming into fruition. What individual should respond to the risk with the preplanned risk response

- A. Project sponsor
- B. Risk owner
- C. Diane
- D. Subject matter expert

Answer: B

NEW QUESTION 209

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 213

Which of the following refers to a process that is used for implementing information security

- A. Classic information security model
- B. Certification and Accreditation (C&A)
- C. Information Assurance (IA)
- D. Five Pillars model

Answer: B

NEW QUESTION 218

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.

- A. Risk Adjustments
- B. Security Certification and Accreditation (C&A)
- C. Vulnerability Assessment and Penetration Testing
- D. Change and Configuration Control

Answer: ABC

NEW QUESTION 219

Fill in the blanks with an appropriate phrase. The is the process of translating system requirements into detailed function criteri a.

- A. functional analysis

Answer: A

NEW QUESTION 223

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

Answer: ABC

NEW QUESTION 226

The Concept of Operations (CONOPS) is a document describing the characteristics of a proposed system from the viewpoint of an individual who will use that system. Which of the following points are included in CONOPS Each correct answer represents a complete solution. Choose all that apply.

- A. Strategies, tactics, policies, and constraints affecting the system
- B. Organizations, activities, and interactions among participants and stakeholders
- C. Statement of the structure of the system
- D. Clear statement of responsibilities and authorities delegated
- E. Statement of the goals and objectives of the system

Answer: ABDE

NEW QUESTION 229

.....

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](#)