ISC2

Exam Questions ISSEP

ISSEP Information Systems Security Engineering Professional

NEW QUESTION 1
Which of the following statements define the role of the ISSEP during the development of the detailed security design, as mentioned in the IATF document Each correct answer represents a complete solution. Choose all that apply.

A. It identifies the information protection problems that needs to be solved.
B. It allocates security mechanisms to system security design elements.
C. It identifies custom security products.
D. It identifies candidate commercial off-the-shelf (COTS)government off-the-shelf (GOTS) security products.

Answer: BCD

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
Fill in the blanks with an appropriate phrase. A is an approved build of the product, and can be a single component or a combination of components.

A. development baseline

Answer: A

NEW QUESTION 5
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 6
Which of the following is a subset discipline of Corporate Governance focused on information security systems and their performance and risk management

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

Answer: C

NEW QUESTION 7
You work as a systems engineer for BlueWell Inc. You want to communicate the quantitative and qualitative system characteristics to all stakeholders. Which of the following documents will you use to achieve the above task

A. IMM
B. CONOPS
C. IPP
D. System Security Context

Answer: B

NEW QUESTION 8

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 9
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 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 are tested and reviewed

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

Answer: A

NEW QUESTION 10
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 12
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 15
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 20
Which of the following roles is also known as the accreditor

A. Data owner
B. Chief Information Officer
C. Chief Risk Officer
D. Designated Approving Authority

Answer: D

NEW QUESTION 25
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 30
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 31
You work as a security engineer for BlueWell Inc. According to you, which of the following DITSCAPNIACAP model phases occurs at the initiation of the project, or at the initial C&A effort of a legacy system

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

Answer: B

NEW QUESTION 32
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 37
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 40
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 45
Part of your change management plan details what should happen in the change control system for your project. Theresa, a junior project manager, asks what the configuration management activities are for scope changes. You tell her that all of the following are valid configuration management activities except for which one

A. Configuration Item Costing
B. Configuration Identification
C. Configuration Verification and Auditing
D. Configuration Status Accounting

Answer: A

NEW QUESTION 49
Which of the following agencies is responsible for funding the development of many technologies such as computer networking, as well as NLS

A. DARPA
B. DTIC
C. DISA

D. DIAP

Answer: A

NEW QUESTION 54
You work as an ISSE for BlueWell Inc. You want to break down user roles, processes, and information until ambiguity is reduced to a satisfactory degree. Which of the following tools will help you to perform the above task

A. PERT Chart
B. Gantt Chart
C. Functional Flow Block Diagram
D. Information Management Model (IMM)

Answer: D

NEW QUESTION 55
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 57
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 58
Which of the following is NOT an objective of the security program

A. Security education
B. Information classification
C. Security organization
D. Security plan

Answer: D

NEW QUESTION 60
Which of the following are the major tasks of risk management Each correct answer represents a complete solution. Choose two.

A. Risk identification
B. Building Risk free systems
C. Assuring the integrity of organizational data
D. Risk control

Answer: AD

NEW QUESTION 65
Which of the following CNSS policies describes the national policy on securing voice communications

A. NSTISSP N
B. 6
C. NSTISSP N
D. 7
E. NSTISSP N
F. 101
G. NSTISSP N
H. 200

Answer: C

NEW QUESTION 68
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 70
Which of the following cooperative programs carried out by NIST provides a nationwide network of local centers offering technical and business assistance to small manufacturers

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

Answer: C

NEW QUESTION 72
Which of the following sections of the SEMP template defines the project constraints, to include constraints on funding, personnel, facilities, manufacturing capability and capacity, critical resources, and other constraints

A. Section 3.1.5
B. Section 3.1.8
C. Section 3.1.9
D. Section 3.1.7

Answer: B

NEW QUESTION 77
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 82
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 84
Which of the following processes provides guidance to the system designers and form the basis of major events in the acquisition phases, such as testing the products for system integration

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

Answer: A

NEW QUESTION 88
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

Answer: B

NEW QUESTION 90
Which of the following phases of NIST SP 800-37 C&A methodology examines the residual risk for acceptability, and prepares the final security accreditation package

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

Answer: D

NEW QUESTION 91
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 92
Which of the following federal laws establishes roles and responsibilities for information security, risk management, testing, and training, and authorizes NIST and NSA to provide guidance for security planning and implementation

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

Answer: B

NEW QUESTION 95
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 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 high integrity and medium availability

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

Answer: B

NEW QUESTION 104
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 109
Under which of the following CNSS policies, NIACAP is mandatory for all the systems that process USG classified information

A. NSTISSP N
B. 11
C. NSTISSP N
D. 101
E. NSTISSP N
F. 7
G. NSTISSP N
H. 6

Answer: D

NEW QUESTION 112

Which of the following describes a residual risk as the risk remaining after a risk mitigation has occurred

A. SSAA
B. ISSO
C. DAA
D. DIACAP

Answer: D

NEW QUESTION 114
Which of the following Registration Tasks sets up the business or operational functional description and system identification

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

Answer: B

NEW QUESTION 116
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
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 124
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 127
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 129
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 132

Which of the following are the most important tasks of the Information Management Plan (IMP) Each correct answer represents a complete solution. Choose all that apply.

A. Define the Information Protection Policy (IPP).
B. Define the System Security Requirements.
C. Define the mission need.
D. Identify how the organization manages its information.

Answer: ACD

NEW QUESTION 136
Which of the following federal agencies provides a forum for the discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of national security systems

A. National Security AgencyCentral Security Service (NSACSS)
B. National Institute of Standards and Technology (NIST)
C. United States Congress
D. Committee on National Security Systems (CNSS)

Answer: D

NEW QUESTION 141
Which of the following Registration Tasks sets up the system architecture description, and describes the C&A boundary

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

Answer: B

NEW QUESTION 146
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 147
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 148
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 152
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 153
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

Answer: A

NEW QUESTION 155
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 157
Which of the following processes provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and the security posture of a system or site

A. ASSET
B. NSA-IAM
C. NIACAP
D. DITSCAP

Answer: C

NEW QUESTION 162
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 164
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 166
Which of the following tasks describes the processes required to ensure that the project includes all the work required, and only the work required, to complete the project successfully

A. Identify Roles and Responsibilities
B. Develop Project Schedule
C. Identify Resources and Availability
D. Estimate project scope

Answer: D

NEW QUESTION 167
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 169
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 171
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 176
Which of the following certification levels requires the completion of the minimum security checklist and more in-depth, independent analysis

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

Answer: A

NEW QUESTION 177
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 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 184
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 185
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 188
Which of the following phases of the ISSE model is used to determine why the system needs to be built and what information needs to be protected

A. Develop detailed security design
B. Define system security requirements
C. Discover information protection needs
D. Define system security architecture

Answer: C

NEW QUESTION 192
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 194
Which of the following email lists is written for the technical audiences, and provides weekly summaries of security issues, new vulnerabilities, potential impact, patches and workarounds, as well as the actions recommended to mitigate risk

A. Cyber Security Tip
B. Cyber Security Alert
C. Cyber Security Bulletin
D. Technical Cyber Security Alert

Answer: C

NEW QUESTION 199
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 200
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 201
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 203
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 204
Fill in the blank with an appropriate phrase. The helps the customer understand and document the information management needs that support the business or

mission.

A. systems engineer

Answer: A

NEW QUESTION 206
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 207
Which of the following is an Information Assurance (IA) model that protects and defends information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation

A. Parkerian Hexad
B. Five Pillars model
C. Capability Maturity Model (CMM)
D. Classic information security model

Answer: B

NEW QUESTION 211
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

ISSEP Practice Exam Features:

* ISSEP Questions and Answers Updated Frequently

* ISSEP Practice Questions Verified by Expert Senior Certified Staff

* ISSEP Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* ISSEP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year