

## CISSP-ISSEP Dumps

### Information Systems Security Engineering Professional

<https://www.certleader.com/CISSP-ISSEP-dumps.html>



**NEW QUESTION 1**

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 2**

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 3**

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 4**

Which of the following Net-Centric Data Strategy goals are required to increase enterprise and community data over private user and system data Each correct answer represents a complete solution. Choose all that apply.

- A. Understandability
- B. Visibility
- C. Interoperability
- D. Accessibility

**Answer:** BD

**NEW QUESTION 5**

Which of the following memorandums directs the Departments and Agencies to post clear privacy policies on World Wide Web sites, and provides guidance for doing it

- A. OMB M-99-18
- B. OMB M-00-13
- C. OMB M-03-19
- D. OMB M-00-07

**Answer:** A

**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 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 9**

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 10**

Which of the following memorandums reminds the departments and agencies of the OMB principles for including and funding security as an element of agency information technology systems and architectures and of the decision criteria which is used to evaluate security for information systems investments

- A. OMB M-00-13
- B. OMB M-99-18
- C. OMB M-00-07
- D. OMB M-03-19

**Answer:** C

**NEW QUESTION 10**

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 11**

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 14**

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 19**

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 23**

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 24**

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 27**

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 29**

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 31**

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 34**

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 39**

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 41**

The Phase 2 of DITSCAP C&A is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. What are the process activities of this phase  
Each correct answer represents a complete solution. Choose all that apply.

- A. Assessment of the Analysis Results
- B. Certification analysis
- C. Registration
- D. System development
- E. Configuring refinement of the SSAA

**Answer:** ABDE

#### NEW QUESTION 46

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 50

The risk transference is referred to the transfer of risks to a third party, usually for a fee, it creates a contractual-relationship for the third party to manage the risk on behalf of the performing organization. Which one of the following is NOT an example of the transference risk response

- A. Warranties
- B. Performance bonds
- C. Use of insurance
- D. Life cycle costing

**Answer:** D

#### NEW QUESTION 51

Your project team has identified a project risk that must be responded to. The risk has been recorded in the risk register and the project team has been discussing potential risk responses for the risk event. The event is not likely to happen for several months but the probability of the event is high. Which one of the following is a valid response to the identified risk event

- A. Earned value management
- B. Risk audit
- C. Corrective action
- D. Technical performance measurement

**Answer:** C

#### NEW QUESTION 56

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 60

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 62

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 65

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 69

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 73

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 74

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 75

Which of the following individuals reviews and approves project deliverables from a QA perspective

- A. Information systems security engineer
- B. System owner
- C. Quality assurance manager
- D. Project manager

**Answer:** C

#### NEW QUESTION 77

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 82

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 83**

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 88**

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 91**

You work as a security engineer for BlueWell Inc. You are working on the ISSE model. In which of the following phases of the ISSE model is the system defined in terms of what security is needed

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

**Answer:** D

**NEW QUESTION 92**

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 94**

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 97**

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 102**

Which of the following are the ways of sending secure e-mail messages over the Internet Each correct answer represents a complete solution. Choose two.

- A. PGP
- B. SMIME
- C. TLS
- D. IPSec

**Answer:** AB

**NEW QUESTION 103**

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 104**

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 107**

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 111**

Which of the following organizations assists the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies

- A. NSACSS
- B. OMB
- C. DCAA
- D. NIST

**Answer:** B

**NEW QUESTION 114**

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 115**

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 119**

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 124**

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 125**

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 128**

Continuous Monitoring is the fourth phase of the security certification and accreditation process. What activities are performed in the Continuous Monitoring process Each correct answer represents a complete solution. Choose all that apply.

- A. Status reporting and documentation
- B. Security control monitoring and impact analyses of changes to the information system
- C. Configuration management and control
- D. Security accreditation documentation
- E. Security accreditation decision

**Answer:** ABC

**NEW QUESTION 132**

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 136**

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 139**

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 140**

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 143**

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 147**

In which of the following phases of the interconnection life cycle as defined by NIST SP

800-47 does the participating organizations perform the following tasks Perform preliminary activities. Examine all relevant technical, security and administrative issues. Form an agreement governing the management, operation, and use of the interconnection.

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

**Answer:** C

**NEW QUESTION 151**

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 155**

Which of the following elements of Registration task 4 defines the operating system, database management system, and software applications, and how they will be used

- A. System firmware
- B. System interface
- C. System software
- D. System hardware

**Answer:** C

**NEW QUESTION 156**

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 158**

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 162**

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 167**

Which of the following categories of system specification describes the technical requirements that cover a service, which is performed on a component of the system

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

**Answer:** B

**NEW QUESTION 172**

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 176**

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 178**

Which of the following cooperative programs carried out by NIST encourages performance excellence among U.S. manufacturers, service companies, educational institutions, and healthcare providers

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

**Answer:** B

**NEW QUESTION 181**

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 185**

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 189**

Which of the following acts promote a risk-based policy for cost effective security Each correct answer represents a part of the solution. Choose all that apply.

- A. Clinger-Cohen Act
- B. Lanham Act
- C. Paperwork Reduction Act (PRA)
- D. Computer Misuse Act

**Answer:** AC

**NEW QUESTION 192**

Which of the following policies describes the national policy on the secure electronic messaging service

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

**Answer:** B

**NEW QUESTION 194**

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 195**

Which of the following NIST Special Publication documents provides a guideline on network security testing

- A. NIST SP 800-60
- B. NIST SP 800-37
- C. NIST SP 800-59
- D. NIST SP 800-42
- E. NIST SP 800-53A
- F. NIST SP 800-53

**Answer:** D

**NEW QUESTION 199**

The Phase 4 of DITSCAP C&A is known as Post Accreditation. This phase starts after the system has been accredited in Phase 3. What are the process activities of this phase Each correct answer represents a complete solution. Choose all that apply.

- A. Security operations
- B. Continue to review and refine the SSAA
- C. Change management
- D. Compliance validation
- E. System operations
- F. Maintenance of the SSAA

**Answer:** ACDEF

**NEW QUESTION 201**

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 203**

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 208**

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 210

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 213

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 214

Which of the following elements are described by the functional requirements task Each correct answer represents a complete solution. Choose all that apply.

- A. Coverage
- B. Accuracy
- C. Quality
- D. Quantity

**Answer:** ACD

#### NEW QUESTION 217

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 221

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 222

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 226**

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

**Answer:** BCD

**NEW QUESTION 229**

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 233**

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 235**

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 237**

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 242**

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 246**

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

**NEW QUESTION 248**

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 251**

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 252**

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 257**

Which of the following is a type of security management for computers and networks in order to identify security breaches

- A. IPS
- B. IDS
- C. ASA
- D. EAP

**Answer:** B

**NEW QUESTION 261**

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 262**

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 264**

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 268**

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 271**

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 273**

Which of the following characteristics are described by the DIAP Information Readiness Assessment function Each correct answer represents a complete solution. Choose all that apply.

- A. It performs vulnerabilitythreat analysis assessment.
- B. It provides for entry and storage of individual system data.
- C. It provides data needed to accurately assess IA readiness.
- D. It identifies and generates IA requirements.

**Answer:** ACD

**NEW QUESTION 275**

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 279**

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 284**

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 289**

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 291**

Which of the following acts assigns the Chief Information Officers (CIO) with the responsibility to develop Information Technology Architectures (ITAs) and is also referred to as the Information Technology Management Reform Act (ITMRA)

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

**Answer:** D

**NEW QUESTION 294**

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 297**

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 299**

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 300**

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 304**

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 308**

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 313**

Which of the CNSS policies describes the national policy on certification and accreditation of national security telecommunications and information systems

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

**Answer:** C

**NEW QUESTION 316**

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 320**

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 324**

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 329**

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 334**

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 339**

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 343**

Which of the following security controls is standardized by the Internet Engineering Task Force (IETF) as the primary network layer protection mechanism

- A. Internet Key Exchange (IKE) Protocol
- B. SMIME
- C. Internet Protocol Security (IPSec)
- D. Secure Socket Layer (SSL)

**Answer:** C

**NEW QUESTION 347**

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 348**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your CISSP-ISSEP Exam with Our Prep Materials Via below:**

<https://www.certleader.com/CISSP-ISSEP-dumps.html>