Number: CISSP-ISSEP
Passing Score: 800
Time Limit: 120
File Version: 5.0

Exam Code: CISSP-ISSEP
Exam Name: Information Systems Security Engineering Professional

Exam A

QUESTION 1
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.

Correct Answer: D
Section:

QUESTION 2
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

Correct Answer: B
Section:

QUESTION 3
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

Correct Answer: C
Section:

QUESTION 4
Which of the following is designed to detect unwanted attempts at accessing, manipulating, and disabling of computer systems through the Internet

A. DAS
B. IDS
C. ACL

D. Ipsec

Correct Answer: B
Section:

QUESTION 5
Which of the following cooperative programs carried out by NIST speed ups the development of modern technologies for broad, national benefit by co-funding research and development partnerships with the private sector

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

Correct Answer: B
Section:

QUESTION 6
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

Correct Answer: D, C, B
Section:

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

Correct Answer: B
Section:

QUESTION 8
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.

Correct Answer: C, D, A
Section:

QUESTION 9
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.

Correct Answer: B, A, D
Section:

QUESTION 10
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)

Correct Answer: C
Section:

QUESTION 11
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

Correct Answer: D
Section:

QUESTION 12
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

Correct Answer: C
Section:

QUESTION 13
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.

Correct Answer: D, B, C
Section:

QUESTION 14
SIMULATION
For interactive and self-paced preparation of exam ISSEP, try our practice exams.
Practice exams also include self assessment and reporting features!
Fill in the blank with an appropriate word. _____ has the goal to securely interconnect people and systems independent of time or location.

A. Netcentric

Correct Answer: A
Section:

QUESTION 15
Which of the following configuration management system processes keeps track of the changes so that the latest acceptable configuration specifications are readily available

A. Configuration Identification
B. Configuration Verification and Audit
C. Configuration Status and Accounting
D. Configuration Control

Correct Answer: C
Section:

QUESTION 16
Which of the following phases of DITSCAP includes the activities that are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle

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

Correct Answer: C
Section:

QUESTION 17

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

Correct Answer: A
Section:

QUESTION 18
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

Correct Answer: E, D, B, A
Section:

QUESTION 19
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

Correct Answer: D
Section:

QUESTION 20
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

Correct Answer: A
Section:

QUESTION 21

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)

Correct Answer: B
Section:

QUESTION 22
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)

Correct Answer: B
Section:

QUESTION 23
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

Correct Answer: C
Section:

QUESTION 24
Which of the following elements of Registration task 4 defines the system's external interfaces as well as the purpose of each external interface, and the relationship between the interface and the system

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

Correct Answer: C
Section:

QUESTION 25
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)

Correct Answer: B
Section:

QUESTION 26
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

Correct Answer: C
Section:

QUESTION 27
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

Correct Answer: C
Section:

QUESTION 28
Which of the following processes culminates in an agreement between key players that a system in its current configuration and operation provides adequate protection controls

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

Correct Answer: A
Section:

QUESTION 29
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

Correct Answer: E, A, F, C, D
Section:

QUESTION 30
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

Correct Answer: C
Section:

QUESTION 31
Which of the following tasks obtains the customer agreement in planning the technical effort

A. Task 9
B. Task 11
C. Task 8
D. Task 10

Correct Answer: B
Section:

QUESTION 32
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

Correct Answer: D, E, F, A, B
Section:

QUESTION 33
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

Correct Answer: D, C, A
Section:

QUESTION 34
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

Correct Answer: A
Section:

QUESTION 35
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

Correct Answer: D
Section:

QUESTION 36
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.

Correct Answer: C, D, A
Section:

QUESTION 37
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

Correct Answer: B
Section:

QUESTION 38
SIMULATION
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

Correct Answer: A
Section:

QUESTION 39
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)

Correct Answer: D
Section:

QUESTION 40
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.

Correct Answer: C
Section:

QUESTION 41
According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Which of the following are among the eight areas of IA defined by DoD Each correct answer represents a complete solution. Choose all that apply.

A. DC Security Design & Configuration
B. EC Enclave and Computing Environment
C. VI Vulnerability and Incident Management
D. Information systems acquisition, development, and maintenance

Correct Answer: A, C, B
Section:

QUESTION 42

Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. Which of the following statements are true about Certification and Accreditation Each correct answer represents a complete solution. Choose two.

A. Accreditation is a comprehensive assessment of the management, operational, and technical security controls in an information system.
B. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system.
C. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system.
D. Certification is the official management decision given by a senior agency official to authorize operation of an information system.

Correct Answer: C, B
Section:

QUESTION 43
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

Correct Answer: B
Section:

QUESTION 44
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

Correct Answer: D
Section:

QUESTION 45
What are the subordinate tasks of the Initiate and Plan IA C&A phase of the DIACAP process Each correct answer represents a complete solution. Choose all that apply.

A. Develop DIACAP strategy.
B. Initiate IA implementation plan.
C. Conduct validation activity.
D. Assemble DIACAP team.
E. Register system with DoD Component IA Program.
F. Assign IA controls.

Correct Answer: E, F, D, A, B
Section:

QUESTION 46

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

Correct Answer: B
Section:

QUESTION 47
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

Correct Answer: D
Section:

QUESTION 48
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

Correct Answer: B
Section:

QUESTION 49
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

Correct Answer: B
Section:

QUESTION 50

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

Correct Answer: A
Section:

QUESTION 51
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

Correct Answer: A
Section:

QUESTION 52
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

Correct Answer: B
Section:

QUESTION 53
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.

Correct Answer: B, D, C
Section:

QUESTION 54
Which of the following individuals is responsible for the oversight of a program that is supported by a team of people that consists of, or be exclusively comprised of contractors

A. Quality Assurance Manager
B. Senior Analyst
C. System Owner
D. Federal program manager

Correct Answer: D
Section:

QUESTION 55
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

Correct Answer: C
Section:

QUESTION 56
You work as a system engineer for BlueWell Inc. You want to verify that the build meets its data requirements, and correctly generates each expected display and report. Which of the following tests will help you to perform the above task

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

Correct Answer: A
Section:

QUESTION 57
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

Correct Answer: B
Section:

QUESTION 58
Which of the following policies describes the national policy on the secure electronic messaging service

A. NSTISSP No. 11

B. NSTISSP No. 7
C. NSTISSP No. 6
D. NSTISSP No. 101

Correct Answer: B
Section:

QUESTION 59
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

Correct Answer: C
Section:

QUESTION 60
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.

Correct Answer: D, B, C
Section:

QUESTION 61
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

Correct Answer: B
Section:

QUESTION 62
Which of the following persons in an organization is responsible for rejecting or accepting the residual risk for a system

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

Correct Answer: C
Section:

QUESTION 63
Which of the following assessment methodologies defines a six-step technical security evaluation

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

Correct Answer: C
Section:

QUESTION 64
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.

Correct Answer: D, C, B
Section:

QUESTION 65
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

Correct Answer: D
Section:

QUESTION 66
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

Correct Answer: C
Section:

QUESTION 67
SIMULATION 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

Correct Answer: A
Section:

QUESTION 68
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

Correct Answer: D
Section:

QUESTION 69
TQM recognizes that quality of all the processes within an organization contribute to the quality of the product. Which of the following are the most important activities in the Total Quality Management Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: B, D, A
Section:

QUESTION 70
SIMULATION
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

Correct Answer: A
Section:

QUESTION 71
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

Correct Answer: A
Section:

QUESTION 72
Your company is covered under a liability insurance policy, which provides various liability coverage for information security risks, including any physical damage of assets, hacking attacks, etc. Which of the following risk management techniques is your company using

A. Risk acceptance
B. Risk mitigation
C. Risk avoidance
D. Risk transfer

Correct Answer: D
Section:

QUESTION 73
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.

Correct Answer: A, B, D
Section:

QUESTION 74
Which of the following approaches can be used to build a security program Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: D, C
Section:

QUESTION 75
SIMULATION
Fill in the blank with the appropriate phrase. _____ provides instructions and directions for completing the Systems Security Authorization Agreement (SSAA).

A. DoDI 5200.40

Correct Answer: A
Section:

QUESTION 76
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

Correct Answer: C, A
Section:

QUESTION 77
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

Correct Answer: B
Section:

QUESTION 78
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

Correct Answer: D
Section:

QUESTION 79
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

Correct Answer: B
Section:

QUESTION 80
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

Correct Answer: D
Section:

QUESTION 81
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

Correct Answer: B
Section:

QUESTION 82
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

Correct Answer: D
Section:

QUESTION 83
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

Correct Answer: A
Section:

QUESTION 84
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

Correct Answer: B, C, D, E
Section:

QUESTION 85
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

Correct Answer: C
Section:

QUESTION 86
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

Correct Answer: B
Section:

QUESTION 87
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

Correct Answer: D
Section:

QUESTION 88
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

Correct Answer: E
Section:

QUESTION 89
Which of the following CNSS policies describes the national policy on controlled access protection

A. NSTISSP No. 101
B. NSTISSP No. 200
C. NCSC No. 5
D. CNSSP No. 14

Correct Answer: B
Section:

QUESTION 90
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

Correct Answer: A
Section:

QUESTION 91
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

Correct Answer: D
Section:

QUESTION 92
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

Correct Answer: D
Section:

QUESTION 93
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

Correct Answer: B
Section:

QUESTION 94
SIMULATION Fill in the blank with an appropriate phrase. A _____ is defined as any activity that has an effect on defining, designing, building, or executing a task, requirement, or procedure.

A. technical effort

Correct Answer: A
Section:

QUESTION 95
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)

Correct Answer: D
Section:

QUESTION 96
Which of the following federal laws are related to hacking activities Each correct answer represents a complete solution. Choose three.

A. 18 U.S.C. 1030
B. 18 U.S.C. 1029
C. 18 U.S.C. 2510
D. 18 U.S.C. 1028

Correct Answer: C, B, A
Section:

QUESTION 97
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

Correct Answer: D
Section:

QUESTION 98
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.

Correct Answer: A, C, D
Section:

QUESTION 99
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

Correct Answer: D
Section:

QUESTION 100
Which of the following are the phases of the Certification and Accreditation (C&A) process Each correct answer represents a complete solution. Choose two.

A. Auditing
B. Initiation
C. Continuous Monitoring
D. Detection

Correct Answer: B, C
Section:

QUESTION 101
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

Correct Answer: A
Section:

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

Correct Answer: A, B
Section:

QUESTION 103
Which of the following federal agencies coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produces foreign intelligence information

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

Correct Answer: B
Section:

QUESTION 104
Which of the following firewall types operates at the Network layer of the OSI model and can filter data by port, interface address, source address, and destination address

A. Circuit-level gateway
B. Application gateway
C. Proxy server
D. Packet Filtering

Correct Answer: D
Section:

QUESTION 105
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

Correct Answer: A, B, D
Section:

QUESTION 106
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)

Correct Answer: A
Section:

QUESTION 107
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

Correct Answer: A
Section:

QUESTION 108
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

Correct Answer: D
Section:

QUESTION 109
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

Correct Answer: B

Section:

QUESTION 110
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)

Correct Answer: A
Section:

QUESTION 111
A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. Which of the following are required to be addressed in a well designed policy Each correct answer represents a part of the solution. Choose all that apply.

A. What is being secured
B. Who is expected to comply with the policy
C. Where is the vulnerability, threat, or risk
D. Who is expected to exploit the vulnerability

Correct Answer: A, B, C
Section:

QUESTION 112
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

Correct Answer: B
Section:

QUESTION 113
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

Correct Answer: D

Section:

QUESTION 114
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

Correct Answer: C
Section:

QUESTION 115
SIMULATION
Fill in the blanks with an appropriate phrase. The_____ is the process of translating system requirements into detailed function criteri a.

A. functional analysis

Correct Answer: A
Section:

QUESTION 116
Which of the CNSS policies describes the national policy on certification and accreditation of national security telecommunications and information systems

A. NSTISSP No. 7
B. NSTISSP No. 11
C. NSTISSP No. 6
D. NSTISSP No. 101

Correct Answer: C
Section:

QUESTION 117
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)

Correct Answer: A
Section:

QUESTION 118

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

Correct Answer: C
Section:

QUESTION 119
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

Correct Answer: D
Section:

QUESTION 120
Which of the following terms describes the security of an information system against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users or the provision of service to unauthorized users

A. Information Assurance (IA)
B. Information Systems Security Engineering (ISSE)
C. Information Protection Policy (IPP)
D. Information systems security (InfoSec)

Correct Answer: D
Section:

QUESTION 121
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

Correct Answer: C
Section:

QUESTION 122

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

A. CNSSP No. 14
B. NCSC No. 5
C. NSTISSP No. 6
D. NSTISSP No. 7

Correct Answer: B
Section:

QUESTION 123
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

Correct Answer: B
Section:

QUESTION 124
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

Correct Answer: A
Section:

QUESTION 125
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

Correct Answer: C
Section:

QUESTION 126
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

Correct Answer: C
Section:

QUESTION 127
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

Correct Answer: D
Section:

QUESTION 128
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

Correct Answer: D, C, A
Section:

QUESTION 129
Which of the following is the acronym of RTM

A. Resource tracking method
B. Requirements Testing Matrix
C. Requirements Traceability Matrix
D. Resource timing method

Correct Answer: C
Section:

QUESTION 130
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

Correct Answer: D
Section:

QUESTION 131
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)

Correct Answer: B
Section:

QUESTION 132
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

Correct Answer: B
Section:

QUESTION 133
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.

Correct Answer: A, D, B
Section:

QUESTION 134
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

Correct Answer: C
Section:

QUESTION 135
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

Correct Answer: D
Section:

QUESTION 136
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

Correct Answer: B
Section:

QUESTION 137
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

Correct Answer: D
Section:

QUESTION 138
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

Correct Answer: B
Section:

QUESTION 139
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

Correct Answer: B
Section:

QUESTION 140
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

Correct Answer: B
Section:

QUESTION 141
Which of the following is a 1996 United States federal law, designed to improve the way the federal government acquires, uses, and disposes information technology

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

Correct Answer: B
Section:

QUESTION 142
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

Correct Answer: A, B, C
Section:

QUESTION 143
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

Correct Answer: C
Section:

QUESTION 144
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

Correct Answer: D
Section:

QUESTION 145
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

Correct Answer: A, B, C
Section:

QUESTION 146
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

Correct Answer: C
Section:

QUESTION 147
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

Correct Answer: A
Section:

QUESTION 148
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

Correct Answer: C, B, A
Section:

QUESTION 149
Which of the following types of CNSS issuances establishes criteria, and assigns responsibilities

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

Correct Answer: D
Section: