CISSP-ISSEP

Number: CISSP-ISSEP
Passing Score: 800
Time Limit: 120 min
File Version: 1

CISSP-ISSEP

https://www.gratisexam.com/

Exam A

QUESTION 1
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
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: (none)
Explanation

Explanation/Reference:

QUESTION 4
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: (none)
Explanation

Explanation/Reference:

QUESTION 5
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: (none)
Explanation

Explanation/Reference:

QUESTION 6
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: (none)
Explanation

Explanation/Reference:

QUESTION 7
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: (none)
Explanation

Explanation/Reference:

QUESTION 8
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: (none)
Explanation

Explanation/Reference:

QUESTION 9
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: (none)
Explanation

Explanation/Reference:

QUESTION 10
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: (none)
Explanation

Explanation/Reference:

QUESTION 11
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: DEFAB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
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: DCA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
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: (none)
Explanation

Explanation/Reference:

QUESTION 14
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: (none)
Explanation

Explanation/Reference:

QUESTION 15
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: CDA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
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: (none)
Explanation

Explanation/Reference:

QUESTION 17
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: (none)
Explanation

Explanation/Reference:

QUESTION 18
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: ACB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
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: CB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
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: (none)
Explanation

Explanation/Reference:

QUESTION 21
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: (none)
Explanation

Explanation/Reference:

QUESTION 22
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: EFDAB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
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: (none)
Explanation

Explanation/Reference:

QUESTION 24
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: (none)
Explanation

Explanation/Reference:

QUESTION 25
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: (none)
Explanation

Explanation/Reference:

QUESTION 26
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: (none)
Explanation

Explanation/Reference:

QUESTION 27
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: BDC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
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: (none)
Explanation

Explanation/Reference:

QUESTION 29
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: (none)
Explanation

Explanation/Reference:

QUESTION 30
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: (none)
Explanation

Explanation/Reference:

QUESTION 31
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: DBC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
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: (none)
Explanation

Explanation/Reference:

QUESTION 33
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: (none)
Explanation

Explanation/Reference:

QUESTION 34
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: (none)
Explanation

Explanation/Reference:

QUESTION 35
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: (none)
Explanation

Explanation/Reference:

QUESTION 36
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: (none)
Explanation

Explanation/Reference:

QUESTION 37
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: (none)
Explanation

Explanation/Reference:

QUESTION 38
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: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
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: (none)
Explanation

Explanation/Reference:

QUESTION 40
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: (none)
Explanation

Explanation/Reference:

QUESTION 41
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: (none)
Explanation

Explanation/Reference:

QUESTION 42
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: (none)
Explanation

Explanation/Reference:

QUESTION 43
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: (none)
Explanation

Explanation/Reference:

QUESTION 44
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: (none)
Explanation

Explanation/Reference:

QUESTION 45
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: BCDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
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: (none)
Explanation

Explanation/Reference:

QUESTION 47
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: (none)
Explanation

Explanation/Reference:

QUESTION 48
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: (none)
Explanation

Explanation/Reference:

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 51
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: (none)
Explanation

Explanation/Reference:

QUESTION 52
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: CBA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
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: CDA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
The principle of the SEMP is not to repeat the information, but rather to ensure that there are processes in place to conduct those functions. Which of the following sections of the SEMP template describes the work authorization procedures as well as change management approval processes

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
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

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 56
Which of the following DITSCAP C&A phases takes place between the signing of the initial version of the SSAA and the formal accreditation of the system

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
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

Correct Answer: BFED
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
NIST SP 800-53A defines three types of interview depending on the level of assessment conducted. Which of the following NIST SP 800-53A interviews consists of informal and ad hoc interviews

A. Abbreviated
B. Significant
C. Substantial
D. Comprehensive

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Which of the following processes provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and the security posture of a system or site

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

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which of the following is NOT an objective of the security program

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise. What are the responsibilities of a Chief Information Officer Each correct answer represents a complete solution. Choose all that apply.

A. Proposing the information technology needed by an enterprise to achieve its goals and then working within a budget to implement the plan
B. Preserving high-level communications and working group relationships in an organization
C. Establishing effective continuous monitoring program for the organization
D. Facilitating the sharing of security risk-related information among authorizing officials

Correct Answer: CBA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which of the following is a temporary approval to operate based on an assessment of the implementation status of the assigned IA Controls

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
System Authorization is the risk management process. System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. What are the different phases of System Authorization Plan Each correct answer represents a part of the solution. Choose all that apply.

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

Correct Answer: EABD
Section: (none)

Explanation

Explanation/Reference:

QUESTION 71
Which of the following CNSS policies describes the national policy on securing voice communications

A. NSTISSP No. 6
B. NSTISSP No. 7
C. NSTISSP No. 101
D. NSTISSP No. 200

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
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: (none)
Explanation

Explanation/Reference:

QUESTION 73
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: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
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: (none)
Explanation

Explanation/Reference:

QUESTION 75
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: (none)
Explanation

Explanation/Reference:

QUESTION 76
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: (none)
Explanation

Explanation/Reference:

QUESTION 77
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: (none)
Explanation

Explanation/Reference:

QUESTION 78
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: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
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: (none)
Explanation

Explanation/Reference:

QUESTION 80
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: (none)
Explanation

Explanation/Reference:

QUESTION 81
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: (none)
Explanation

Explanation/Reference:

QUESTION 82
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: DCB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
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: (none)
Explanation

Explanation/Reference:

QUESTION 84
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: CDA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
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: BAD
Section: (none)

Explanation

Explanation/Reference:

QUESTION 86
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: (none)
Explanation

Explanation/Reference:

QUESTION 87
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: (none)
Explanation

Explanation/Reference:

QUESTION 88
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: (none)
Explanation

Explanation/Reference:

QUESTION 89
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: (none)
Explanation

Explanation/Reference:

QUESTION 90
Which of the following individuals is responsible for monitoring the information system environment for factors that can negatively impact the security of the system and its accreditation

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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 91
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: (none)
Explanation

Explanation/Reference:

QUESTION 92
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: ADB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
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: (none)
Explanation

Explanation/Reference:

QUESTION 94
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: (none)
Explanation

Explanation/Reference:

QUESTION 95
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: (none)

Explanation

Explanation/Reference:

QUESTION 96
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: (none)
Explanation

Explanation/Reference:

QUESTION 97
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: (none)
Explanation

Explanation/Reference:

QUESTION 98
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: (none)
Explanation

Explanation/Reference:

QUESTION 99
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: CBA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
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: (none)
Explanation

Explanation/Reference:

QUESTION 101
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: (none)
Explanation

Explanation/Reference:

QUESTION 102
Which of the following techniques are used after a security breach and are intended to limit the extent of any damage caused by the incident

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
Under which of the following CNSS policies, NIACAP is mandatory for all the systems that process USG classified information

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
Which of the following terms describes the measures that protect and support information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
Which of the following is an Information Assurance (IA) model that protects and defends information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
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

Correct Answer: BAC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
FIPS 199 defines the three levels of potential impact on organizations low, moderate, and high. Which of the following are the effects of loss of confidentiality, integrity, or availability in a high level potential impact

A. The loss of confidentiality, integrity, or availability might cause severe degradation in or loss of mission capability to an extent.
B. The loss of confidentiality, integrity, or availability might result in major financial losses.
C. The loss of confidentiality, integrity, or availability might result in a major damage to organizational assets.
D. The loss of confidentiality, integrity, or availability might result in severe damages like life threatening injuries or loss of life.

Correct Answer: ACBD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
Which of the following are the benefits of SE as stated by MIL-STD-499B Each correct answer represents a complete solution. Choose all that apply.

A. It develops work breakdown structures and statements of work.
B. It establishes and maintains configuration management of the system.
C. It develops needed user training equipment, procedures, and data.
D. It provides high-quality products and services, with the correct people and performance features, at an affordable price, and on time.

Correct Answer: CBA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
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: (none)
Explanation

Explanation/Reference:

QUESTION 113
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: CBA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
Which of the following are the major tasks of risk management Each correct answer represents a complete solution. Choose two.

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

Correct Answer: AD
Section: (none)

Explanation

Explanation/Reference:

QUESTION 116
You are working as a project manager in your organization. You are nearing the final stages of project execution and looking towards the final risk monitoring and controlling activities. For your project archives, which one of the following is an output of risk monitoring and control

A. Quantitative risk analysis
B. Risk audits
C. Requested changes
D. Qualitative risk analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
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

Correct Answer: CBA
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
Which of the following organizations incorporates building secure audio and video communications equipment, making tamper protection products, and providing trusted microelectronics solutions

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference: