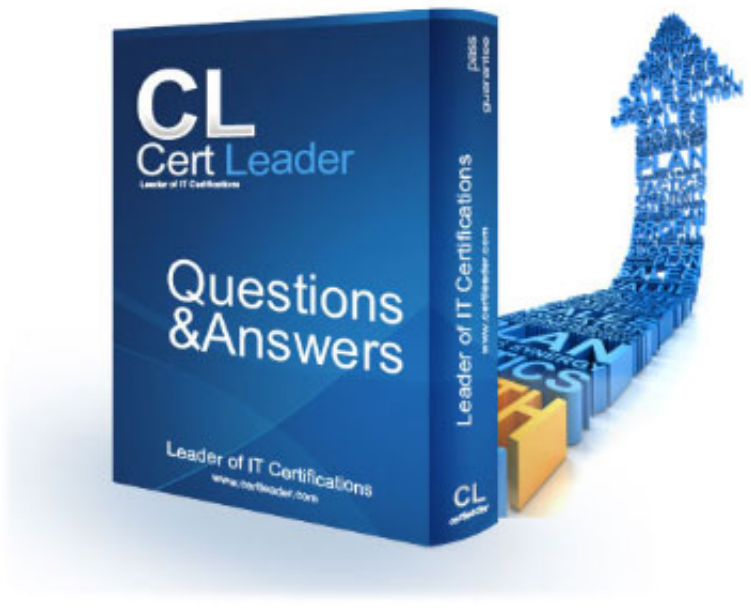
CISSP-ISSEP Dumps

Information Systems Security Engineering Professional

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



NEW QUESTION 1
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

Answer: CD

NEW QUESTION 2
Which of the following DoD policies provides assistance on how to implement policy,
assign responsibilities, and prescribe procedures for applying integrated, layered protection of the DoD information systems and networks

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

Answer: D

NEW QUESTION 3
Which of the following statements define the role of the ISSEP during the development of the detailed security design, as mentioned in the IATF document Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BCD

NEW QUESTION 4
Which of the following are the functional analysis and allocation tools Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ACD

NEW QUESTION 5
System Authorization is the risk management process. System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. What are the different phases of System Authorization Plan Each correct answer represents a part of the solution. Choose all that apply.

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

Answer: ABDE

NEW QUESTION 6
Which of the following documents contains the threats to the information management, and the security services and controls required to counter those threats

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

Answer: B

NEW QUESTION 7
Which of the following acts is used to recognize the importance of information security to the economic and national security interests of the United States

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

Answer: B

NEW QUESTION 8
Which of the following memorandums directs the Departments and Agencies to post clear privacy policies on World Wide Web sites, and provides guidance for doing it

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

Answer: A

NEW QUESTION 9
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

Answer: B

NEW QUESTION 10
FIPS 199 defines the three levels of potential impact on organizations. Which of the following potential impact levels shows limited adverse effects on organizational operations, organizational assets, or individuals

A. Moderate
B. Medium
C. High
D. Low

Answer: D

NEW QUESTION 10
Fill in the blanks with an appropriate phrase. A is an approved build of the product, and can be a single component or a combination of components.

A. development baseline

Answer: A

NEW QUESTION 11
Which of the following types of cryptography defined by FIPS 185 describes a cryptographic algorithm or a tool accepted by the National Security Agency for protecting sensitive, unclassified information in the systems as stated in Section 2315 of Title 10, United States Code

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

Answer: B

NEW QUESTION 13
Which of the following NIST documents describes that minimizing negative impact on an organization and a need for sound basis in decision making are the fundamental reasons organizations implement a risk management process for their IT systems

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

Answer: B

NEW QUESTION 14
Which of the following cooperative programs carried out by NIST conducts research to advance the nation's technology infrastructure

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

Answer: B

NEW QUESTION 16
Which of the following memorandums reminds the departments and agencies of the OMB principles for including and funding security as an element of agency information technology systems and architectures and of the decision criteria which is used to evaluate security for information systems investments

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

Answer: C

NEW QUESTION 21
Which of the following is a standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system

A. SSAA
B. TCSEC
C. FIPS
D. FITSAF

Answer: B

NEW QUESTION 26
Your project has several risks that may cause serious financial impact should they happen. You have studied the risk events and made some potential risk responses for the risk events but management wants you to do more. They'd like for you to create some type of a chart that identified the risk probability and impact with a financial amount for each risk event. What is the likely outcome of creating this type of chart

A. Risk response plan
B. Quantitative analysis
C. Risk response
D. Contingency reserve

Answer: D

NEW QUESTION 29
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

Answer: ABD

NEW QUESTION 30
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

Answer: B

NEW QUESTION 31
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

Answer: C

NEW QUESTION 35
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

Answer: B

NEW QUESTION 39
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)

Answer: D

NEW QUESTION 40
Fill in the blank with the appropriate phrase. The is the risk that remains after the implementation of new or enhanced controls.

A. residual risk

Answer: A

NEW QUESTION 41
Fill in the blank with an appropriate section name. is a section of the SEMP template, which specifies the methods and reasoning planned to build the requisite trade-offs between functionality, performance, cost, and risk.

A. System Analysis

Answer: A

NEW QUESTION 42
You work as a security engineer for BlueWell Inc. Which of the following documents will you use as a guide for the security certification and accreditation of Federal Information Systems

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

Answer: B

NEW QUESTION 45
FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls are tested and reviewed

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

Answer: A

NEW QUESTION 48
The Phase 2 of DITSCAP C&A is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. What are the process activities of this phase Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABDE

NEW QUESTION 53
You work as a security engineer for BlueWell Inc. According to you, which of the following statements determines the main focus of the ISSE process

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

Answer: B

NEW QUESTION 57
You work as a systems engineer for BlueWell Inc. You are working on translating system requirements into detailed function criteria. Which of the following diagrams will help you to show all of the function requirements and their groupings in one diagram

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

Answer: C

NEW QUESTION 61
Which of the following areas of information system, as separated by Information Assurance Framework, is a collection of local computing devices, regardless of physical location, that are interconnected via local area networks (LANs) and governed by a single security policy

A. Networks and Infrastructures
B. Supporting Infrastructures
C. Enclave Boundaries
D. Local Computing Environments

Answer: C

NEW QUESTION 62
Which of the following types of cryptography defined by FIPS 185 describes a cryptographic algorithm or a tool accepted by the National Security Agency for protecting classified information

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

Answer: D

NEW QUESTION 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.

Answer: BCD

NEW QUESTION 69
What are the responsibilities of a system owner Each correct answer represents a complete solution. Choose all that apply.

A. Integrates security considerations into application and system purchasing decisions and development projects.
B. Ensures that the necessary security controls are in place.
C. Ensures that adequate security is being provided by the necessary controls, password management, remote access controls, operating system configurations, and so on.
D. Ensures that the systems are properly assessed for vulnerabilities and must report any to the incident response team and data owner.

Answer: ACD

NEW QUESTION 74
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.

Answer: BC

NEW QUESTION 76
Which of the following federal agencies has the objective to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life

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

Answer: A

NEW QUESTION 79
You work as a security engineer for BlueWell Inc. According to you, which of the following DITSCAPNIACAP model phases occurs at the initiation of the project, or at the initial C&A effort of a legacy system

A. Post Accreditation
B. Definition

C. Verification
D. Validation

Answer: B

NEW QUESTION 82
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

Answer: D

NEW QUESTION 83
Which of the following individuals reviews and approves project deliverables from a QA perspective

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

Answer: C

NEW QUESTION 87
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

Answer: B

NEW QUESTION 88
There are seven risk responses for any project. Which one of the following is a valid risk response for a negative risk event

A. Acceptance
B. Enhance
C. Share
D. Exploit

Answer: A

NEW QUESTION 89
Which of the following tasks prepares the technical management plan in planning the technical effort

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

Answer: B

NEW QUESTION 94
Fill in the blank with an appropriate phrase. seeks to improve the quality of process outputs by identifying and removing the causes of defects and variability in manufacturing and business processes.

A. Six Sigma

Answer: A

NEW QUESTION 99
Part of your change management plan details what should happen in the change control system for your project. Theresa, a junior project manager, asks what the configuration management activities are for scope changes. You tell her that all of the following are valid configuration management activities except for which one

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

Answer: A

NEW QUESTION 102
You work as a security engineer for BlueWell Inc. You are working on the ISSE model. In
which of the following phases of the ISSE model is the system defined in terms of what security is needed

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

Answer: D

NEW QUESTION 107
Which of the following agencies is responsible for funding the development of many technologies such as computer networking, as well as NLS

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

Answer: A

NEW QUESTION 112
You work as an ISSE for BlueWell Inc. You want to break down user roles, processes, and information until ambiguity is reduced to a satisfactory degree. Which of the following tools will help you to perform the above task

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

Answer: D

NEW QUESTION 117
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)

Answer: D

NEW QUESTION 118
John works as a security engineer for BlueWell Inc. He wants to identify the different functions that the system will need to perform to meet the documented missionbusiness needs. Which of the following processes will John use to achieve the task

A. Modes of operation
B. Performance requirement
C. Functional requirement
D. Technical performance measures

Answer: C

NEW QUESTION 122
Which of the following are the ways of sending secure e-mail messages over the Internet Each correct answer represents a complete solution. Choose two.

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

Answer: AB

NEW QUESTION 126
Which of the following individuals informs all C&A participants about life cycle actions, security requirements, and documented user needs

A. User representative
B. DAA
C. Certification Agent
D. IS program manager

Answer: D

NEW QUESTION 130
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

Answer: ABC

NEW QUESTION 132
In which of the following DIACAP phases is residual risk analyzed

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

Answer: E

NEW QUESTION 134
Which of the following organizations assists the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies

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

Answer: B

NEW QUESTION 137
Which of the following processes illustrate the study of a technical nature of interest to focused audience, and consist of interim or final reports on work made by NIST for external
sponsors, including government and non-government sponsors

A. Federal Information Processing Standards (FIPS)
B. Special Publication (SP)
C. NISTIRs (Internal Reports)
D. DIACAP

Answer: C

NEW QUESTION 138
Which of the following individuals is responsible for monitoring the information system
environment for factors that can negatively impact the security of the system and its accreditation

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

Answer: D

NEW QUESTION 140
Fill in the blank with an appropriate phrase. is used to verify and accredit systems by making a standard process, set of activities, general tasks, and management structure.

A. DITSCAPNIACAP

Answer: A

NEW QUESTION 144
Which of the following statements is true about residual risks

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

Answer: C

NEW QUESTION 146

Which of the following agencies provides command and control capabilities and enterprise infrastructure to continuously operate and assure a global net-centric enterprise in direct support to joint warfighters, National level leaders, and other mission and coalition partners
across the full spectrum of operations

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

Answer: C

NEW QUESTION 147
DoD 8500.2 establishes IA controls for information systems according to the Mission Assurance Categories (MAC) and confidentiality levels. Which of the following MAC levels requires basic integrity and availability

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

Answer: D

NEW QUESTION 150
Which of the following processes provides guidance to the system designers and form the basis of major events in the acquisition phases, such as testing the products for system integration

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

Answer: A

NEW QUESTION 154
Which of the following federal laws is designed to protect computer data from theft

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

Answer: B

NEW QUESTION 158
Which of the following types of CNSS issuances establishes or describes policy and programs, provides authority, or assigns responsibilities

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

Answer: B

NEW QUESTION 159
Which of the following memorandums reminds the Federal agencies that it is required by law and policy to establish clear privacy policies for Web activities and to comply with those policies

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

Answer: D

NEW QUESTION 164
In which of the following phases of the interconnection life cycle as defined by NIST SP
800-47 does the participating organizations perform the following tasks Perform preliminary activities. Examine all relevant technical, security and administrative issues. Form an agreement governing the management, operation, and use of the interconnection.

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

Answer: C

NEW QUESTION 169
Which of the following phases of NIST SP 800-37 C&A methodology examines the residual risk for acceptability, and prepares the final security accreditation package

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

Answer: D

NEW QUESTION 172
Which of the following elements of Registration task 4 defines the operating system, database management system, and software applications, and how they will be used

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

Answer: C

NEW QUESTION 175
Which of the following assessment methodologies defines a six-step technical security evaluation

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

Answer: C

NEW QUESTION 178
You work as a systems engineer for BlueWell Inc. You want to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. Which of the following processes will you use to accomplish the task

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

Answer: A

NEW QUESTION 181
In 2003, NIST developed a new Certification & Accreditation (C&A) guideline known as FIPS 199. What levels of potential impact are defined by FIPS 199 Each correct answer represents a complete solution. Choose all that apply.

A. High
B. Medium
C. Low
D. Moderate

Answer: ABC

NEW QUESTION 186
Which of the following agencies serves the DoD community as the largest central resource for DoD and government-funded scientific, technical, engineering, and business related information available today

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

Answer: C

NEW QUESTION 188
Which of the following DITSCAPNIACAP model phases is used to show the required evidence to support the DAA in accreditation process and conclude in an Approval To Operate (ATO)

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

Answer: B

NEW QUESTION 189
Which of the following refers to an information security document that is used in the United States Department of Defense (DoD) to describe and accredit networks and systems

A. SSAA
B. FITSAF
C. FIPS
D. TCSEC

Answer: A

NEW QUESTION 194
Which of the following cooperative programs carried out by NIST encourages performance excellence among U.S. manufacturers, service companies, educational institutions, and healthcare providers

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

Answer: B

NEW QUESTION 197
Under which of the following CNSS policies, NIACAP is mandatory for all the systems that process USG classified information

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

Answer: D

NEW QUESTION 199
Which of the following describes a residual risk as the risk remaining after a risk mitigation has occurred

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

Answer: D

NEW QUESTION 204
You work as a system engineer for BlueWell Inc. Which of the following documents will help you to describe the detailed plans, procedures, and schedules to guide the transition process

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

Answer: B

NEW QUESTION 205
Which of the following acts promote a risk-based policy for cost effective security Each correct answer represents a part of the solution. Choose all that apply.

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

Answer: AC

NEW QUESTION 207
Fill in the blank with an appropriate phrase. The process is used for allocating performance and designing the requirements to each function.

A. functional allocation

Answer: A

NEW QUESTION 209

An Authorizing Official plays the role of an approver. What are the responsibilities of an Authorizing Official Each correct answer represents a complete solution. Choose all that apply.

A. Ascertaining the security posture of the organization's information system
B. Reviewing security status reports and critical security documents
C. Determining the requirement of reauthorization and reauthorizing information systems when required
D. Establishing and implementing the organization's continuous monitoring program

Answer: ABC

NEW QUESTION 214
The Phase 4 of DITSCAP C&A is known as Post Accreditation. This phase starts after the system has been accredited in Phase 3. What are the process activities of this phase Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ACDEF

NEW QUESTION 219
Which of the following are the most important tasks of the Information Management Plan (IMP) Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ACD

NEW QUESTION 223
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

Answer: D

NEW QUESTION 226
Which of the following laws is the first to implement penalties for the creator of viruses, worms, and other types of malicious code that causes harm to the computer systems

A. Computer Fraud and Abuse Act
B. Computer Security Act
C. Gramm-Leach-Bliley Act
D. Digital Millennium Copyright Act

Answer: A

NEW QUESTION 228
Which of the following federal agencies provides a forum for the discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of national security systems

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

Answer: D

NEW QUESTION 230
Which of the following Registration Tasks sets up the system architecture description, and describes the C&A boundary

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

Answer: B

NEW QUESTION 232
Numerous information security standards promote good security practices and define frameworks or systems to structure the analysis and design for managing information security controls. Which of the following are the U.S. Federal Government information security standards Each correct answer represents a complete solution. Choose all that apply.

A. CA Certification, Accreditation, and Security Assessments
B. Information systems acquisition, development, and maintenance
C. IR Incident Response
D. SA System and Services Acquisition

Answer: ACD

NEW QUESTION 233
Which of the following is used to indicate that the software has met a defined quality level and is ready for mass distribution either by electronic means or by physical media

A. ATM
B. RTM
C. CRO
D. DAA

Answer: B

NEW QUESTION 234
Which of the following categories of system specification describes the technical, performance, operational, maintenance, and support characteristics for the entire system

A. Process specification
B. Product specification
C. Development specification
D. System specification

Answer: D

NEW QUESTION 237
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

Answer: ABC

NEW QUESTION 241
The functional analysis process is used for translating system requirements into detailed function criteria. Which of the following are the elements of functional analysis process Each correct answer represents a complete solution. Choose all that apply.

A. Model possible overall system behaviors that are needed to achieve the system requirements.
B. Develop concepts and alternatives that are not technology or component bound.
C. Decompose functional requirements into discrete tasks or activities, the focus is still on technology not functions or components.
D. Use a top-down with some bottom-up approach verification.

Answer: ABD

NEW QUESTION 244
Registration Task 5 identifies the system security requirements. Which of the following elements of Registration Task 5 defines the type of data processed by the system

A. Data security requirement
B. Network connection rule
C. Applicable instruction or directive
D. Security concept of operation

Answer: A

NEW QUESTION 247
What NIACAP certification levels are recommended by the certifier Each correct answer represents a complete solution. Choose all that apply.

A. Basic System Review
B. Basic Security Review
C. Maximum Analysis
D. Comprehensive Analysis
E. Detailed Analysis
F. Minimum Analysis

Answer: BDEF

NEW QUESTION 250
Della works as a security engineer for BlueWell Inc. She wants to establish configuration management and control procedures that will document proposed or actual changes to the information system. Which of the following phases of NIST SP 800-37 C&A methodology will define the above task

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

Answer: D

NEW QUESTION 255
Certification and Accreditation (C&A or CnA) is a process for implementing information security. Which of the following is the correct order of C&A phases in a DITSCAP assessment

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

Answer: D

NEW QUESTION 260
Which of the following types of cryptography defined by FIPS 185 describes a cryptographic algorithm or a tool accepted as a Federal Information Processing Standard

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

Answer: B

NEW QUESTION 265
Which of the following professionals plays the role of a monitor and takes part in the organization's configuration management process

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

Answer: C

NEW QUESTION 268
According to which of the following DoD policies, the implementation of DITSCAP is mandatory for all the systems that process both DoD classified and unclassified information?

A. DoD 8500.2
B. DoDI 5200.40
C. DoD 8510.1-M DITSCAP
D. DoD 8500.1 (IAW)

Answer: D

NEW QUESTION 272
You work as a security manager for BlueWell Inc. You are going through the NIST SP 800- 37 C&A methodology, which is based on four well defined phases. In which of the following phases of NIST SP 800-37 C&A methodology does the security categorization occur

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

Answer: B

NEW QUESTION 275
You work as a Network Administrator for PassGuide Inc. You need to secure web services of your company in order to have secure transactions. Which of the following will you recommend for providing security

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

Answer: D

NEW QUESTION 278
Which of the following organizations incorporates building secure audio and video communications equipment, making tamper protection products, and providing trusted microelectronics solutions

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

Answer: B

NEW QUESTION 280
Which of the following tasks describes the processes required to ensure that the project includes all the work required, and only the work required, to complete the project successfully

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

Answer: D

NEW QUESTION 283
Which of the following is a type of security management for computers and networks in order to identify security breaches

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

Answer: B

NEW QUESTION 284
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

Answer: ABC

NEW QUESTION 289
Which of the following guidelines is recommended for engineering, protecting, managing, processing, and controlling national security and sensitive (although unclassified) information

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

Answer: B

NEW QUESTION 294
Which of the following DITSCAPNIACAP model phases is used to confirm that the evolving system development and integration complies with the agreements between role players documented in the first phase

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

Answer: A

NEW QUESTION 297
Which of the following certification levels requires the completion of the minimum security checklist and more in-depth, independent analysis

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

Answer: A

NEW QUESTION 299
Which of the following techniques are used after a security breach and are intended to limit the extent of any damage caused by the incident

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

Answer: A

NEW QUESTION 303
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

Answer: A

NEW QUESTION 304
Della works as a systems engineer for BlueWell Inc. She wants to convert system requirements into a comprehensive function standard, and break the higher-level functions into lower-level functions. Which of the following processes will Della use to accomplish the task

A. Risk analysis
B. Functional allocation
C. Functional analysis
D. Functional baseline

Answer: C

NEW QUESTION 309
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

Answer: A

NEW QUESTION 312
Which of the following are the subtasks of the Define Life-Cycle Process Concepts task Each correct answer represents a complete solution. Choose all that apply.

A. Training
B. Personnel
C. Control
D. Manpower

Answer: ABD

NEW QUESTION 317
Which of the following acts assigns the Chief Information Officers (CIO) with the responsibility to develop Information Technology Architectures (ITAs) and is also referred to as the Information Technology Management Reform Act (ITMRA)

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

Answer: D

NEW QUESTION 320
Which of the following documents is defined as a source document, which is most useful for the ISSE when classifying the needed security functionality

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

Answer: A

NEW QUESTION 321
Which of the following Registration Tasks notifies the DAA, Certifier, and User Representative that the system requires C&A Support

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

Answer: D

NEW QUESTION 323
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

Answer: C

NEW QUESTION 325
Which of the following organizations incorporates building secure audio and video communications equipment, making tamper protection products, and providing trusted microelectronics solutions

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

Answer: B

NEW QUESTION 327
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.

Answer: ABC

NEW QUESTION 332
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

Answer: A

NEW QUESTION 334
Which of the following responsibilities are executed by the federal program manager

A. Ensure justification of expenditures and investment in systems engineering activities.
B. Coordinate activities to obtain funding.
C. Review project deliverables.
D. Review and approve project plans.

Answer: ABD

NEW QUESTION 338
Which of the following email lists is written for the technical audiences, and provides weekly summaries of security issues, new vulnerabilities, potential impact, patches and workarounds, as well as the actions recommended to mitigate risk

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

Answer: C

NEW QUESTION 341
Which of the following DoD directives is referred to as the Defense Automation Resources Management Manual

A. DoD 8910.1
B. DoD 7950.1-M
C. DoD 5200.22-M
D. DoD 5200.1-R
E. DoDD 8000.1

Answer: B

NEW QUESTION 342
Which of the CNSS policies describes the national policy on certification and accreditation of national security telecommunications and information systems

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

Answer: C

NEW QUESTION 345
The phase 3 of the Risk Management Framework (RMF) process is known as mitigation planning. Which of the following processes take place in phase 3 Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABD

NEW QUESTION 347
FIPS 199 defines the three levels of potential impact on organizations low, moderate, and high. Which of the following are the effects of loss of confidentiality, integrity, or availability in a high level potential impact

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

Answer: ABCD

NEW QUESTION 351
Which of the following NIST Special Publication documents provides a guideline on questionnaires and checklists through which systems can be evaluated for compliance against specific control objectives

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

Answer: D

NEW QUESTION 352
Which of the following DoD policies establishes IA controls for information systems according to the Mission Assurance Categories (MAC) and confidentiality levels

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

Answer: B

NEW QUESTION 356
Your project is an agricultural-based project that deals with plant irrigation systems. You have discovered a byproduct in your project that your organization could use to make a profit. If your organization seizes this opportunity it would be an example of what risk response

A. Enhancing
B. Positive
C. Opportunistic
D. Exploiting

Answer: D

NEW QUESTION 360
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

Answer: C

NEW QUESTION 362
Which of the following refers to a process that is used for implementing information security

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

Answer: B

NEW QUESTION 364
The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum standard process for the certification and accreditation of computer and
telecommunications systems that handle U.S. national security information. What are the different types of NIACAP accreditation Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABC

NEW QUESTION 365
Which of the following security controls is standardized by the Internet Engineering Task Force (IETF) as the primary network layer protection mechanism

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

Answer: C

NEW QUESTION 367
The Concept of Operations (CONOPS) is a document describing the characteristics of a proposed system from the viewpoint of an individual who will use that system. Which of the following points are included in CONOPS Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABDE

NEW QUESTION 370
Which of the following is an Information Assurance (IA) model that protects and defends information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation

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

Answer: B

NEW QUESTION 372
Which of the following CNSS policies describes the national policy on controlled access protection

A. NSTISSP N
B. 101
C. NSTISSP N
D. 200
E. NCSC N
F. 5

G. CNSSP N
H. 14

Answer: B

NEW QUESTION 375
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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