ISC.Cissp-issep.v2018-02-24.q201

Exam Code:	CISSP-ISSEP
Exam Name:	CISSP-ISSEP - Information Systems Security Engineering Professional
Certification Provider:	ISC
Free Question Number:	201
Version:	v2018-02-24
# of views:	1002
# of Questions views:	69702
https://www.freecram.net/torrent/ISC.Cissp-issep.v2018-02-24.q201.html	

NEW QUESTION: 1
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. Application gateway
B. Proxy server
C. Circuit-level gateway
D. Packet Filtering
Answer: D (LEAVE A REPLY)

NEW QUESTION: 2
Which of the following Registration Tasks sets up the system architecture description, and describes the C&A boundary
A. Registration Task 1
B. Registration Task 2
C. Registration Task 3
D. Registration Task 4
Answer: (SHOW ANSWER)

NEW QUESTION: 3
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 Protection Policy (IPP)
B. Information Assurance (IA)
C. Information systems security (InfoSec)

D. Information Systems Security Engineering (ISSE)
Answer: (SHOW ANSWER)

NEW QUESTION: 4
SIMULATION
Fill in the blank with an appropriate phrase. A _____ is defined as any activity that has an effect on defining, designing, building, or executing a task, requirement, or procedure.
Answer:
technical effort

NEW QUESTION: 5
SIMULATION
Fill in the blank with an appropriate phrase. The _____ helps the customer understand and document the information management needs that support the business or mission.
Answer:
systems engineer

NEW QUESTION: 6
Which of the following Security Control Assessment Tasks evaluates the operational, technical, and the management security controls of the information system using the techniques and measures selected or developed
A. Security Control Assessment Task 1
B. Security Control Assessment Task 4
C. Security Control Assessment Task 3
D. Security Control Assessment Task 2
Answer: (SHOW ANSWER)

NEW QUESTION: 7
SIMULATION
Fill in the blanks with an appropriate phrase. The_____ is the process of translating system requirements into detailed function criteri a.
Answer:
functional analysis

NEW QUESTION: 8
Which of the following types of CNSS issuances establishes or describes policy and programs, provides authority, or assigns responsibilities
A. Policies
B. Instructions
C. Advisory memoranda
D. Directives

Answer: D (LEAVE A REPLY)

NEW QUESTION: 9
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-00-13
B. OMB M-03-19
C. OMB M-00-07
D. OMB M-99-18
Answer: (SHOW ANSWER)

NEW QUESTION: 10
A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. What are the different types of policies Each correct answer represents a complete solution. Choose all that apply.

A. Regulatory
B. Systematic
C. Advisory
D. Informative
Answer: (SHOW ANSWER)

NEW QUESTION: 11
Which of the following guidelines is recommended for engineering, protecting, managing, processing, and controlling national security and sensitive (although unclassified) information
A. Special Publication (SP)
B. NISTIRs (Internal Reports)
C. DIACAP by the United States Department of Defense (DoD)
D. Federal Information Processing Standard (FIPS)
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Which of the following documents contains the threats to the information management, and the security services and controls required to counter those threats
A. Information Protection Policy (IPP)
B. IMM
C. CONOPS
D. System Security Context
Answer: (SHOW ANSWER)

NEW QUESTION: 13

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: (SHOW ANSWER)

Explanation/Reference:

NEW QUESTION: 14

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 800-60

B. NIST Special Publication 800-53

C. NIST Special Publication 800-59

D. NIST Special Publication 800-37

Answer: (SHOW ANSWER)

NEW QUESTION: 15

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

A. Functional hierarchy diagram

B. Timeline analysis diagram

C. Functional flow block diagram (FFBD)

D. Activity diagram

Answer: (SHOW ANSWER)

NEW QUESTION: 16

Which of the following roles is also known as the accreditor

A. Chief Risk Officer

B. Data owner

C. Chief Information Officer

D. Designated Approving Authority

Answer: (SHOW ANSWER)

NEW QUESTION: 17
Which of the following acts is endorsed to provide a clear statement of the proscribed activity concerning computers to the law enforcement community, those who own and operate computers, and those tempted to commit crimes by unauthorized access to computers
A. Computer Fraud and Abuse Act
B. Government Information Security Reform Act (GISRA)
C. Computer Security Act
D. Federal Information Security Management Act (FISMA)
Answer: (SHOW ANSWER)

NEW QUESTION: 18
Which of the following organizations is a USG initiative designed to meet the security testing, evaluation, and assessment needs of both information technology (IT) producers and consumers
A. CNSS
B. NSA
C. NIAP
D. NIST
Answer: (SHOW ANSWER)

NEW QUESTION: 19
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. Configuration management and control
B. Status reporting and documentation
C. Security accreditation documentation E. Security accreditation decision
D. Security control monitoring and impact analyses of changes to the information system
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 20
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-03-19
C. OMB M-00-07

D. OMB M-99-18
Answer: (SHOW ANSWER)

NEW QUESTION: 21
Which of the following processes culminates in an agreement between key players that a system in its current configuration and operation provides adequate protection controls
A. Information systems security engineering (ISSE)
B. Information Assurance (IA)
C. Risk Management
D. Certification and accreditation (C&A)
Answer: (SHOW ANSWER)

NEW QUESTION: 22
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: (SHOW ANSWER)

NEW QUESTION: 23
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, Validation, Definition, and Post Accreditation
C. Verification, Definition, Validation, and Post Accreditation
D. Definition, Verification, Validation, and Post Accreditation
Answer: (SHOW ANSWER)

NEW QUESTION: 24
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. DIACAP
B. Federal Information Processing Standards (FIPS)
C. Special Publication (SP)
D. NISTIRs (Internal Reports)
Answer: (SHOW ANSWER)

NEW QUESTION: 25

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 2

C. Registration Task 1

D. Registration Task 3

Answer: (SHOW ANSWER)

NEW QUESTION: 26

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. Initiation

C. Continuous Monitoring

D. Security Accreditation

Answer: (SHOW ANSWER)

NEW QUESTION: 27

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. Change and Configuration Control

B. Risk Adjustments

C. Vulnerability Assessment and Penetration Testing

D. Security Certification and Accreditation (C&A)

Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 28

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

Answer: (SHOW ANSWER)

NEW QUESTION: 29

What are the responsibilities of a system owner Each correct answer represents a complete solution.

Choose all that apply.

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

NEW QUESTION: 30
Which of the following refers to a process that is used for implementing information security
A. Five Pillars model
B. Information Assurance (IA)
C. Certification and Accreditation (C&A)
D. Classic information security model
Answer: (SHOW ANSWER)

NEW QUESTION: 31
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. Committee on National Security Systems (CNSS)
B. National Security Agency (NSA)
C. United States Congress
D. National Institute of Standards and Technology (NIST)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 32
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. Computer Fraud and Abuse Act
B. Computer Misuse Act
C. FISMA

D. Lanham Act
Answer: (SHOW ANSWER)

NEW QUESTION: 33
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 800-53
B. NIST Special Publication 800-37
C. NIST Special Publication 800-60
D. NIST Special Publication 800-37A
E. NIST Special Publication 800-53A
F. NIST Special Publication 800-59
Answer: (SHOW ANSWER)

NEW QUESTION: 34
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. Validation
B. Verification
C. Post accreditation
D. Definition
Answer: (SHOW ANSWER)

NEW QUESTION: 35
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 mission need.
C. Define the System Security Requirements.
D. Identify how the organization manages its information.
Answer: (SHOW ANSWER)

NEW QUESTION: 36
Which of the following is a temporary approval to operate based on an assessment of the implementation status of the assigned IA Controls
A. DATO
B. IATT
C. IATO
D. ATO
Answer: (SHOW ANSWER)

NEW QUESTION: 37
Which of the following responsibilities are executed by the federal program manager
A. Coordinate activities to obtain funding.
B. Review and approve project plans.
C. Review project deliverables.
D. Ensure justification of expenditures and investment in systems engineering activities.
Answer: (SHOW ANSWER)

NEW QUESTION: 38
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. Secure accreditation
D. System accreditation
Answer: (SHOW ANSWER)

NEW QUESTION: 39
Under which of the following CNSS policies, NIACAP is mandatory for all the systems that process USG classified information
A. NSTISSP No. 101
B. NSTISSP No. 7
C. NSTISSP No. 11
D. NSTISSP No. 6
Answer: (SHOW ANSWER)

NEW QUESTION: 40
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 800-60
B. NIST SP 800-53
C. NIST SP 800-30
D. NIST SP 800-37
Answer: (SHOW ANSWER)

NEW QUESTION: 41

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 requirements

B. Define system security architecture

C. Discover information protection needs

D. Develop detailed security design

Answer: (SHOW ANSWER)

NEW QUESTION: 42

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. Capability Maturity Model (CMM)

B. Five Pillars model

C. Parkerian Hexad

D. Classic information security model

Answer: (SHOW ANSWER)

NEW QUESTION: 43

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. Detective controls

B. Preventive controls

C. Corrective controls

D. Safeguards

Answer: (SHOW ANSWER)

NEW QUESTION: 44

SIMULATION

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.

Answer:

DITSCAPNIACAP

NEW QUESTION: 45

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

A. NSTISSP No. 6

B. NSTISSP No. 200

C. NSTISSP No. 101

D. NSTISSP No. 7
Answer: C (LEAVE A REPLY)

NEW QUESTION: 46
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. Transition plan
B. Configuration management plan
C. Acquisition plan
D. Systems engineering management plan (SEMP)
Answer: (SHOW ANSWER)

NEW QUESTION: 47
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. Paperwork Reduction Act (PRA)
B. Clinger-Cohen Act
C. Lanham Act
D. Computer Misuse Act
Answer: (SHOW ANSWER)

NEW QUESTION: 48
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 Verification and Auditing
C. Configuration Identification
D. Configuration Status Accounting
Answer: (SHOW ANSWER)

NEW QUESTION: 49
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. FITSAF
B. TCSEC
C. SSAA
D. FIPS
Answer: (SHOW ANSWER)

NEW QUESTION: 50
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. Reviewing security status reports and critical security documents
B. Establishing and implementing the organization's continuous monitoring program
C. Ascertaining the security posture of the organization's information system
D. Determining the requirement of reauthorization and reauthorizing information systems when required
Answer: (SHOW ANSWER)

NEW QUESTION: 51
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. System development
B. Registration
C. Assessment of the Analysis Results
D. Certification analysis
E. Configuring refinement of the SSAA
Answer: (SHOW ANSWER)

NEW QUESTION: 52
Which of the following types of CNSS issuances describes how to implement the policy or prescribes the manner of a policy
A. Instructions
B. Advisory memoranda
C. Directives
D. Policies
Answer: (SHOW ANSWER)

NEW QUESTION: 53

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

A. NIST SP 800-42

B. NIST SP 800-59

C. NIST SP 800-60

D. NIST SP 800-53A

E. NIST SP 800-37

F. NIST SP 800-53

Answer: (SHOW ANSWER)

NEW QUESTION: 54

Which of the following phases of the ISSE model is used to determine why the system needs to be built and what information needs to be protected

A. Discover information protection needs

B. Define system security requirements

C. Define system security architecture

D. Develop detailed security design

Answer: (SHOW ANSWER)

NEW QUESTION: 55

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. Digital Millennium Copyright Act

D. Gramm-Leach-Bliley Act

Answer: (SHOW ANSWER)

NEW QUESTION: 56

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. Personnel

B. Training

C. Manpower

D. Control

Answer: (SHOW ANSWER)

NEW QUESTION: 57

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. IMM

B. CONOPS
C. System Security Context
D. Information Protection Policy (IPP)
Answer: (SHOW ANSWER)

NEW QUESTION: 58
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. Security Certification
B. Security Accreditation
C. Continuous Monitoring
D. Initiation
Answer: (SHOW ANSWER)

NEW QUESTION: 59
SIMULATION
For interactive and self-paced preparation of exam ISSEP, try our practice exams.
Practice exams also include self assessment and reporting features!
Fill in the blank with an appropriate word. _____ has the goal to securely interconnect people and systems independent of time or location.
Answer:
Netcentric

NEW QUESTION: 60
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 800-59
B. NIST SP 800-37
C. NIST SP 800-60
D. NIST SP 800-53A
E. NIST SP 800-53
F. NIST SP 800-26
Answer: (SHOW ANSWER)

NEW QUESTION: 61
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. DAA
B. CRO
C. ATM
D. RTM

Answer: (SHOW ANSWER)

NEW QUESTION: 62
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 Protection Policy (IPP)
B. Information Assurance (IA)
C. Statistical process control (SPC)
D. Information management model (IMM)
Answer: (SHOW ANSWER)

NEW QUESTION: 63
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. United States Congress
C. National Security AgencyCentral Security Service (NSACSS)
D. Committee on National Security Systems (CNSS)
Answer: (SHOW ANSWER)

NEW QUESTION: 64
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. Moderate
C. Medium
D. Low
Answer: (SHOW ANSWER)

NEW QUESTION: 65

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

A. Risk control

B. Building Risk free systems

C. Risk identification

D. Assuring the integrity of organizational data

Answer: (SHOW ANSWER)

NEW QUESTION: 66

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. Internet Protocol Security (IPSec)

C. Common data security architecture (CDSA)

D. Application program interface (API)

Answer: (SHOW ANSWER)

NEW QUESTION: 67

SIMULATION

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

Answer:

residual risk

NEW QUESTION: 68

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. Life cycle costing

D. Use of insurance

Answer: C (LEAVE A REPLY)

NEW QUESTION: 69

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

A. Detection

B. Auditing

C. Initiation
D. Continuous Monitoring
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 70
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 (E) cryptography
B. Type I cryptography
C. Type III cryptography
D. Type II cryptography
Answer: (SHOW ANSWER)

NEW QUESTION: 71
SIMULATION
Fill in the blank with an appropriate section name. _____ is a section of the SEMP template, which specifies the methods and reasoning planned to build the requisite trade-offs between functionality, performance, cost, and risk.
Answer:
System Analysis

NEW QUESTION: 72
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. Who is expected to comply with the policy
B. Where is the vulnerability, threat, or risk
C. Who is expected to exploit the vulnerability
D. What is being secured
Answer: (SHOW ANSWER)

NEW QUESTION: 73
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 2
D. Level 3
E. Level 1

Answer: (SHOW ANSWER)

NEW QUESTION: 74
Which of the following DoD policies establishes policies and assigns responsibilities to achieve DoD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network-centric warfare
A. DoD 8500.2 Information Assurance Implementation
B. DoD 8500.1 Information Assurance (IA)
C. DoD 8510.1-M DITSCAP
D. DoDI 5200.40
Answer: B (LEAVE A REPLY)

NEW QUESTION: 75
Which of the following organizations incorporates building secure audio and video communications equipment, making tamper protection products, and providing trusted microelectronics solutions
A. DARPA
B. DTIC
C. DIAP
D. NSA IAD
Answer: (SHOW ANSWER)

NEW QUESTION: 76
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. Maintenance of quality
B. Quality costs
C. Quality improvements
D. Quality renewal
Answer: (SHOW ANSWER)

NEW QUESTION: 77
What NIACAP certification levels are recommended by the certifier Each correct answer represents a complete solution. Choose all that apply.
A. Minimum Analysis
B. Detailed Analysis
C. Basic Security Review
D. Maximum Analysis
E. Basic System Review
F. Comprehensive Analysis
Answer: A,B,C,F (LEAVE A REPLY)

NEW QUESTION: 78
Which of the following federal laws establishes roles and responsibilities for information security, risk management, testing, and training, and authorizes NIST and NSA to provide guidance for security planning and implementation
A. Computer Fraud and Abuse Act
B. Federal Information Security Management Act (FISMA)
C. Computer Security Act
D. Government Information Security Reform Act (GISRA)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 79
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. Execute and update IA implementation plan.
D. Conduct validation activities.
Answer: (SHOW ANSWER)

NEW QUESTION: 80
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. Performance requirements
C. Human factors
D. Functional requirements
Answer: A (LEAVE A REPLY)

NEW QUESTION: 81
SIMULATION

Fill in the blank with an appropriate phrase. The _____ process is used for allocating performance and designing the requirements to each function.
Answer:
functional allocation

NEW QUESTION: 82
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. Medium
B. Low
C. Moderate
D. High
Answer: (SHOW ANSWER)

NEW QUESTION: 83
Which of the following CNSS policies describes the national policy on controlled access protection
A. NCSC No. 5
B. NSTISSP No. 101
C. CNSSP No. 14
D. NSTISSP No. 200
Answer: (SHOW ANSWER)

NEW QUESTION: 84
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. Document and implement a mitigation plan.
D. Identify threats, vulnerabilities, and controls that will be evaluated.
Answer: (SHOW ANSWER)

NEW QUESTION: 85
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. IS program manager

D. Certification Agent
Answer: (SHOW ANSWER)

NEW QUESTION: 86
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 8510.1-M DITSCAP
B. DoD 8500.2
C. DoD 8500.1 (IAW)
D. DoDI 5200.40
Answer: C (LEAVE A REPLY)

NEW QUESTION: 87
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 software
B. System interface
C. System firmware
D. System hardware
Answer: (SHOW ANSWER)

NEW QUESTION: 88
In which of the following DIACAP phases is residual risk analyzed
A. Phase 3
B. Phase 2
C. Phase 5
D. Phase 4
E. Phase 1
Answer: (SHOW ANSWER)

NEW QUESTION: 89
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. Development specification
C. System specification
D. Product specification
Answer: (SHOW ANSWER)

NEW QUESTION: 90

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

A. Registration Task 1
B. Registration Task 3
C. Registration Task 4
D. Registration Task 2
Answer: (SHOW ANSWER)

NEW QUESTION: 91
Which of the following cooperative programs carried out by NIST conducts research to advance the nation's technology infrastructure
A. Advanced Technology Program
B. Manufacturing Extension Partnership
C. NIST Laboratories
D. Baldrige National Quality Program
Answer: (SHOW ANSWER)

NEW QUESTION: 92
Which of the following agencies is responsible for funding the development of many technologies such as computer networking, as well as NLS
A. DTIC
B. DARPA
C. DIAP
D. DISA
Answer: (SHOW ANSWER)

NEW QUESTION: 93
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. NIACAP
B. DITSCAP

C. NSA-IAM
D. ASSET
Answer: A (LEAVE A REPLY)

NEW QUESTION: 94
Which of the following types of CNSS issuances establishes criteria, and assigns responsibilities
A. Instructions
B. Policies
C. Directives
D. Advisory memoranda
Answer: (SHOW ANSWER)

NEW QUESTION: 95
Which of the following individuals is an upper-level manager who has the power and capability to evaluate the mission, business case, and budgetary needs of the system while also considering the security risks
A. Program Manager
B. User Representative
C. DAA
D. Certifier
Answer: (SHOW ANSWER)

NEW QUESTION: 96
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 Resources and Availability
B. Identify Roles and Responsibilities
C. Develop Project Schedule
D. Estimate project scope
Answer: (SHOW ANSWER)

NEW QUESTION: 97
In which of the following phases of the interconnection life cycle as defined by NIST SP 800-47, do the organizations build and execute a plan for establishing the interconnection, including executing or configuring appropriate security controls
A. Establishing the interconnection
B. Maintaining the interconnection
C. Disconnecting the interconnection
D. Planning the interconnection
Answer: (SHOW ANSWER)

NEW QUESTION: 98
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 III (E) cryptography
B. Type II cryptography
C. Type III cryptography
D. Type I cryptography
Answer: B (LEAVE A REPLY)

NEW QUESTION: 99
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. Instruct systems engineers on availability, integrity, and confidentiality.
B. Identify the information protection needs.
C. Design information systems that will meet the certification and accreditation documentation.
D. Ensure information systems are designed and developed with functional relevance.
Answer: (SHOW ANSWER)

NEW QUESTION: 100
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. Functional requirement
C. Performance requirement
D. Technical performance measures
Answer: (SHOW ANSWER)

NEW QUESTION: 101
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. Exploiting
B. Positive
C. Opportunistic
D. Enhancing
Answer: (SHOW ANSWER)

NEW QUESTION: 102

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. Application program interface (API)

B. Common data security architecture (CDSA)

C. File encryptors

D. Internet Protocol Security (IPSec)

Answer: (SHOW ANSWER)

NEW QUESTION: 103

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 establishes and maintains configuration management of the system.

B. It provides high-quality products and services, with the correct people and performance features, at an affordable price, and on time.

C. It develops needed user training equipment, procedures, and data.

D. It develops work breakdown structures and statements of work.

Answer: (SHOW ANSWER)

NEW QUESTION: 104

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. DCAA

C. NIST

D. OMB

Answer: (SHOW ANSWER)

NEW QUESTION: 105

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 3.1.7

B. Section 3.1.9

C. Section 3.1.5

D. Section 3.1.8

Answer: (SHOW ANSWER)

NEW QUESTION: 106

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

NEW QUESTION: 107
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 allocates security mechanisms to system security design elements.
B. It identifies candidate commercial off-the-shelf (COTS)government off-the-shelf (GOTS) security products.
C. It identifies the information protection problems that needs to be solved.
D. It identifies custom security products.
Answer: (SHOW ANSWER)

NEW QUESTION: 108
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 IV
B. MAC I
C. MAC III
D. MAC II
Answer: D (LEAVE A REPLY)

NEW QUESTION: 109

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

A. DoDD 8000.1

B. DoD 5200.22-M

C. DoD 8910.1

D. DoD 5200.1-R

E. DoD 7950.1-M

Answer: E (LEAVE A REPLY)

NEW QUESTION: 110

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

A. CL 4

B. CL 3

C. CL 1

D. CL 2

Answer: (SHOW ANSWER)

NEW QUESTION: 111

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. Defending systems

C. Protecting information

D. Providing command and control and situational awareness

Answer: (SHOW ANSWER)

NEW QUESTION: 112

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. Local Computing Environments

B. Networks and Infrastructures

C. Enclave Boundaries

D. Supporting Infrastructures

Answer: (SHOW ANSWER)

NEW QUESTION: 113

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

A. Computer Security Act

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

NEW QUESTION: 114
Which of the following is the acronym of RTM
A. Resource tracking method
B. Requirements Traceability Matrix
C. Requirements Testing Matrix
D. Resource timing method
Answer: (SHOW ANSWER)

NEW QUESTION: 115
Which of the following documents is described in the statement below It is developed along with all processes of the risk management. It contains the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning.
A. Quality management plan
B. Project charter
C. Risk management plan
D. Risk register
Answer: (SHOW ANSWER)

NEW QUESTION: 116
Which of the following certification levels requires the completion of the minimum security checklist, and the system user or an independent certifier can complete the checklist
A. CL 1
B. CL 3
C. CL 4
D. CL 2
Answer: (SHOW ANSWER)

NEW QUESTION: 117
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. Committee on National Security Systems (CNSS)
C. United States Congress
D. National Institute of Standards and Technology (NIST)
Answer: (SHOW ANSWER)

NEW QUESTION: 118
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. System Owner
B. Quality Assurance Manager
C. Federal program manager
D. Senior Analyst
Answer: (SHOW ANSWER)

NEW QUESTION: 119
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. Maintaining the interconnection
B. Establishing the interconnection
C. Disconnecting the interconnection
D. Planning the interconnection
Answer: (SHOW ANSWER)

NEW QUESTION: 120
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. DISA
C. DIAP
D. DTIC
Answer: (SHOW ANSWER)

NEW QUESTION: 121
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 III
B. MAC II
C. MAC IV
D. MAC I
Answer: (SHOW ANSWER)

NEW QUESTION: 122
The Information System Security Officer (ISSO) and Information System Security Engineer (ISSE) play the role of a supporter and advisor, respectively. Which of the following statements are true about ISSO and ISSE Each correct answer represents a complete solution. Choose all that apply.
A. An ISSE provides advice on the impacts of system changes.
B. An ISSO manages the security of the information system that is slated for Certification & Accreditation (C&A).
C. An ISSE provides advice on the continuous monitoring of the information system.
D. An ISSE manages the security of the information system that is slated for Certification & Accreditation (C&A).
E. An ISSO takes part in the development activities that are required to implement system changes.
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 123
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 result in severe damages like life threatening injuries or loss of life.
B. The loss of confidentiality, integrity, or availability might cause severe degradation in or loss of mission capability to an extent.
C. The loss of confidentiality, integrity, or availability might result in major financial losses.
D. The loss of confidentiality, integrity, or availability might result in a major damage to organizational assets.
Answer: (SHOW ANSWER)

NEW QUESTION: 124
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 Bulletin
B. Technical Cyber Security Alert
C. Cyber Security Alert
D. Cyber Security Tip
Answer: (SHOW ANSWER)

NEW QUESTION: 125
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: (SHOW ANSWER)

NEW QUESTION: 126
Which of the following individuals reviews and approves project deliverables from a QA perspective
A. System owner
B. Project manager
C. Information systems security engineer
D. Quality assurance manager
Answer: (SHOW ANSWER)

NEW QUESTION: 127
Which of the following is NOT used in the practice of Information Assurance (IA) to define assurance requirements
A. Parkerian Hexad
B. Communications Management Plan
C. Five Pillars model
D. Classic information security model
Answer: (SHOW ANSWER)

NEW QUESTION: 128
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. Advanced Technology Program
C. Baldrige National Quality Program
D. NIST Laboratories

Answer: (SHOW ANSWER)

NEW QUESTION: 129
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 Security Officer
B. Chief Risk Officer
C. Information System Owner
D. Chief Information Officer
Answer: (SHOW ANSWER)

NEW QUESTION: 130
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 Assurance (IA)
B. Information Systems Security Engineering (ISSE)
C. Information systems security (InfoSec)
D. Information Protection Policy (IPP)
Answer: (SHOW ANSWER)

NEW QUESTION: 131
You work as a systems engineer for BlueWell Inc. You want to communicate the quantitative and qualitative system characteristics to all stakeholders. Which of the following documents will you use to achieve the above task
A. CONOPS
B. IPP
C. System Security Context
D. IMM
Answer: (SHOW ANSWER)

NEW QUESTION: 132
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. Initiation
B. Continuous Monitoring
C. Security Certification
D. Security Accreditation
Answer: (SHOW ANSWER)

NEW QUESTION: 133
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. Manufacturing Extension Partnership
B. NIST Laboratories
C. Advanced Technology Program
D. Baldrige National Quality Program
Answer: (SHOW ANSWER)

NEW QUESTION: 134
Which of the following DITSCAP phases validates that the preceding work has produced an IS that operates in a specified computing environment
A. Phase 4
B. Phase 3
C. Phase 2
D. Phase 1
Answer: (SHOW ANSWER)

NEW QUESTION: 135
SIMULATION
Fill in the blank with the appropriate phrase. _____ provides instructions and directions for completing the Systems Security Authorization Agreement (SSAA).
Answer:
DoDI 5200.40

NEW QUESTION: 136
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 software
C. System hardware
D. System interface
Answer: (SHOW ANSWER)

NEW QUESTION: 137
Which of the following tasks obtains the customer agreement in planning the technical effort
A. Task 9
B. Task 10
C. Task 11
D. Task 8
Answer: (SHOW ANSWER)

NEW QUESTION: 138
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. Baldrige National Quality Program
D. Manufacturing Extension Partnership
Answer: (SHOW ANSWER)

NEW QUESTION: 139
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. Change management
B. System operations
C. Maintenance of the SSAA
D. Continue to review and refine the SSAA
E. Security operations
F. Compliance validation
Answer: (SHOW ANSWER)

NEW QUESTION: 140
There are seven risk responses for any project. Which one of the following is a valid risk response for a negative risk event

A. Share
B. Acceptance
C. Enhance
D. Exploit
Answer: (SHOW ANSWER)

NEW QUESTION: 141
Your project team has identified a project risk that must be responded to. The risk has been recorded in the risk register and the project team has been discussing potential risk responses for the risk event. The event is not likely to happen for several months but the probability of the event is high. Which one of the following is a valid response to the identified risk event
A. Corrective action
B. Risk audit
C. Technical performance measurement
D. Earned value management
Answer: (SHOW ANSWER)

NEW QUESTION: 142
Lisa is the project manager of the SQL project for her company. She has completed the risk response planning with her project team and is now ready to update the risk register to reflect the risk response.
Which of the following statements best describes the level of detail Lisa should include with the risk responses she has created
A. The level of detail must define exactly the risk response for each identified risk.
B. The level of detail is set of project risk governance.
C. The level of detail should correspond with the priority ranking.
D. The level of detail is set by historical information.
Answer: (SHOW ANSWER)

NEW QUESTION: 143
Which of the following describes a residual risk as the risk remaining after a risk mitigation has occurred
A. ISSO
B. DIACAP
C. SSAA
D. DAA
Answer: (SHOW ANSWER)

NEW QUESTION: 144
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. Internet Protocol Security (IPSec)
C. Secure Socket Layer (SSL)
D. SMIME
Answer: (SHOW ANSWER)

NEW QUESTION: 145
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. DISA
B. DIAP
C. DTIC
D. DARPA
Answer: (SHOW ANSWER)

NEW QUESTION: 146
Which of the following types of firewalls increases the security of data packets by remembering the state of connection at the network and the session layers as they pass through the filter
A. Virtual firewall
B. Stateful packet filter firewall
C. PIX firewall
D. Stateless packet filter firewall
Answer: (SHOW ANSWER)

NEW QUESTION: 147
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. Definition
B. Post Accreditation
C. Validation
D. Verification
Answer: (SHOW ANSWER)

NEW QUESTION: 148
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. Computer Misuse Act
B. Lanham Act
C. Paperwork Reduction Act
D. Clinger-Cohen Act
Answer: (SHOW ANSWER)

NEW QUESTION: 149

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

A. AU audit and accountability

B. Organization of information security

C. Risk assessment and treatment

D. Human resources security

Answer: (SHOW ANSWER)

NEW QUESTION: 150

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: (SHOW ANSWER)

NEW QUESTION: 151

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

A. Security plan

B. Security organization

C. Information classification

D. Security education

Answer: (SHOW ANSWER)

NEW QUESTION: 152

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. TCSEC
B. SSAA
C. FITSAF
D. FIPS
Answer: (SHOW ANSWER)

NEW QUESTION: 153
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. Left-Up Approach
B. Top-Down Approach
C. Bottom-Up Approach
D. Right-Up Approach
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 154
Which of the following rated systems of the Orange book has mandatory protection of the TCB
A. D-rated
B. B-rated
C. C-rated
D. A-rated
Answer: (SHOW ANSWER)

NEW QUESTION: 155
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. Comprehensive
C. Substantial
D. Significant
Answer: (SHOW ANSWER)

NEW QUESTION: 156
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. Visibility
B. Accessibility
C. Understandability
D. Interoperability

Answer: (SHOW ANSWER)

NEW QUESTION: 157
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 II cryptography
B. Type I cryptography
C. Type III (E) cryptography
D. Type III cryptography
Answer: (SHOW ANSWER)

NEW QUESTION: 158
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: (SHOW ANSWER)

NEW QUESTION: 159
Which of the following requires all general support systems and major applications to be fully certified and accredited before these systems and applications are put into production Each correct answer represents a part of the solution. Choose all that apply.
A. FIPS
B. Office of Management and Budget (OMB)
C. NIST
D. FISMA
Answer: (SHOW ANSWER)

NEW QUESTION: 160
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. Blowfish
B. SMIME
C. DES
D. PGP
Answer: (SHOW ANSWER)

NEW QUESTION: 161
Which of the following policies describes the national policy on the secure electronic messaging service
A. NSTISSP No. 11
B. NSTISSP No. 6
C. NSTISSP No. 101
D. NSTISSP No. 7
Answer: (SHOW ANSWER)

NEW QUESTION: 162
SIMULATION
Fill in the blank with an appropriate phrase. _____ seeks to improve the quality of process outputs by identifying and removing the causes of defects and variability in manufacturing and business processes.
Answer:
Six Sigma

NEW QUESTION: 163
Which of the CNSS policies describes the national policy on certification and accreditation of national security telecommunications and information systems
A. NSTISSP No. 6
B. NSTISSP No. 11
C. NSTISSP No. 101
D. NSTISSP No. 7
Answer: (SHOW ANSWER)

NEW QUESTION: 164
Which of the following persons in an organization is responsible for rejecting or accepting the residual risk for a system
A. Designated Approving Authority (DAA)
B. Information Systems Security Officer (ISSO)
C. Chief Information Security Officer (CISO)
D. System Owner
Answer: (SHOW ANSWER)

NEW QUESTION: 165
SIMULATION
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.
Answer:

development baseline

NEW QUESTION: 166
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. Risk Analysis
B. Information Systems Security Engineering (ISSE)
C. Risk Management
D. Information Assurance (IA)
Answer: (SHOW ANSWER)

NEW QUESTION: 167
Which of the following DoD directives defines DITSCAP as the standard C&A process for the Department of Defense
A. DoD 8910.1
B. DoD 5200.22-M
C. DoD 5200.40
D. DoD 8000.1
Answer: (SHOW ANSWER)

NEW QUESTION: 168
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 the official management decision given by a senior agency official to authorize operation of an information system.
B. Certification is the official management decision given by a senior agency official to authorize operation of an information system.
C. Accreditation is a comprehensive assessment of the management, operational, and technical security controls in an information system.

D. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system.
Answer: (SHOW ANSWER)

NEW QUESTION: 169
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 provides for entry and storage of individual system data.
B. It identifies and generates IA requirements.
C. It provides data needed to accurately assess IA readiness.
D. It performs vulnerabilitythreat analysis assessment.
Answer: (SHOW ANSWER)

NEW QUESTION: 170
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 3.1.5
C. Section 3.1.7
D. Section 3.1.9
Answer: (SHOW ANSWER)

NEW QUESTION: 171
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. Computer Misuse Act
B. Lanham Act
C. Clinger Cohen Act
D. Paperwork Reduction Act
Answer: (SHOW ANSWER)

NEW QUESTION: 172
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. Requested changes
C. Qualitative risk analysis
D. Risk audits

Answer: (SHOW ANSWER)

NEW QUESTION: 173
Which of the following statements is true about residual risks
A. It is the probabilistic risk before implementing all security measures.
B. It is the probabilistic risk after implementing all security measures.
C. It can be considered as an indicator of threats coupled with vulnerability.
D. It is a weakness or lack of safeguard that can be exploited by a threat.
Answer: (SHOW ANSWER)

NEW QUESTION: 174
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. Authorization
B. Certification
C. Post-certification
D. Post-Authorization
E. Pre-certification
Answer: (SHOW ANSWER)

NEW QUESTION: 175
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. Establishing effective continuous monitoring program for the organization
B. Facilitating the sharing of security risk-related information among authorizing officials
C. Proposing the information technology needed by an enterprise to achieve its goals and then working within a budget to implement the plan
D. Preserving high-level communications and working group relationships in an organization
Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 176
Which of the following principles are defined by the IATF model Each correct answer represents a complete solution. Choose all that apply.
A. The degree to which the security of the system, as it is defined, designed, and implemented, meets the security needs.
B. The problem space is defined by the customer's mission or business needs.

C. The systems engineer and information systems security engineer define the solution space, which is driven by the problem space.
D. Always keep the problem and solution spaces separate.
Answer: (SHOW ANSWER)

NEW QUESTION: 177
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. DoDI 5200.40
C. DoD 8510.1-M DITSCAP
D. DoD 8500.2 Information Assurance Implementation
Answer: (SHOW ANSWER)

NEW QUESTION: 178
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. Applicable instruction or directive
B. Network connection rule
C. Data security requirement
D. Security concept of operation
Answer: (SHOW ANSWER)

NEW QUESTION: 179
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. SMIME
B. HTTP
C. VPN
D. SSL
Answer: (SHOW ANSWER)

NEW QUESTION: 180
Which of the following phases of DITSCAP includes the activities that are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle

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

Answer: A (LEAVE A REPLY)

NEW QUESTION: 181
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. Post accreditation
C. Validation
D. Definition
Answer: (SHOW ANSWER)

NEW QUESTION: 182
Which of the following tools demands involvement by upper executives, in order to integrate quality into the business system and avoid delegation of quality functions to junior administrators
A. ISO 90012000
B. SEI-CMM
C. Six Sigma
D. Benchmarking
Answer: (SHOW ANSWER)

NEW QUESTION: 183
Which of the following is a type of security management for computers and networks in order to identify security breaches
A. ASA
B. EAP
C. IPS
D. IDS
Answer: (SHOW ANSWER)

NEW QUESTION: 184
Which of the following protocols is used to establish a secure terminal to a remote network device

A. WEP
B. SMTP
C. SSH
D. IPSec
Answer: (SHOW ANSWER)

NEW QUESTION: 185
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. Timeline analysis diagram
B. Functional hierarchy diagram
C. Functional flow block diagram (FFBD)
D. Activity diagram
Answer: (SHOW ANSWER)

NEW QUESTION: 186
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. Functional analysis
B. Risk analysis
C. Functional baseline
D. Functional allocation
Answer: (SHOW ANSWER)

NEW QUESTION: 187
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. Organizations, activities, and interactions among participants and stakeholders
B. Statement of the goals and objectives of the system
C. Clear statement of responsibilities and authorities delegated
D. Statement of the structure of the system
E. Strategies, tactics, policies, and constraints affecting the system
Answer: (SHOW ANSWER)

NEW QUESTION: 188

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. Traceability matrix

B. FIPS 199

C. NIST SP 800-50

D. FIPS 200

Answer: (SHOW ANSWER)

NEW QUESTION: 189

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

A. Quantity

B. Accuracy

C. Coverage

D. Quality

Answer: (SHOW ANSWER)

NEW QUESTION: 190

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. Risk response

C. Quantitative analysis

D. Contingency reserve

Answer: (SHOW ANSWER)

NEW QUESTION: 191

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. Regression test

B. Performance test

C. Functional test

D. Reliability test

Answer: (SHOW ANSWER)

NEW QUESTION: 192

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

A. IDS

B. DAS

C. ACL

D. Ipsec

Answer: (SHOW ANSWER)

NEW QUESTION: 193

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. DTIC

B. DIAP

C. DARPA

D. DISA

Answer: (SHOW ANSWER)

NEW QUESTION: 194

Which of the following Security Control Assessment Tasks gathers the documentation and supporting materials essential for the assessment of the security controls in the information system

A. Security Control Assessment Task 4

B. Security Control Assessment Task 1

C. Security Control Assessment Task 3

D. Security Control Assessment Task 2

Answer: B (LEAVE A REPLY)

NEW QUESTION: 195

Which of the following professionals is responsible for starting the Certification & Accreditation (C&A) process

A. Information system owner

B. Authorizing Official

C. Chief Risk Officer (CRO)

D. Chief Information Officer (CIO)

Answer: (SHOW ANSWER)

NEW QUESTION: 196

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 Verification and Audit

B. Configuration Identification
C. Configuration Status and Accounting
D. Configuration Control
Answer: C (LEAVE A REPLY)

NEW QUESTION: 197
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 mitigation
B. Risk transfer
C. Risk acceptance
D. Risk avoidance
Answer: (SHOW ANSWER)

NEW QUESTION: 198
Which of the following professionals plays the role of a monitor and takes part in the organization's configuration management process
A. Senior Agency Information Security Officer
B. Authorizing Official
C. Common Control Provider
D. Chief Information Officer
Answer: (SHOW ANSWER)

NEW QUESTION: 199
Which of the following CNSS policies describes the national policy on use of cryptomaterial by activities operating in high risk environments
A. NSTISSP No. 6
B. CNSSP No. 14
C. NCSC No. 5
D. NSTISSP No. 7
Answer: C (LEAVE A REPLY)

NEW QUESTION: 200

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. Diane

B. Risk owner

C. Subject matter expert

D. Project sponsor

Answer: (SHOW ANSWER)

NEW QUESTION: 201

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-03-19

B. OMB M-01-08

C. OMB M-00-07

D. OMB M-00-13

Answer: (SHOW ANSWER)