ISC2

Exam Questions CISSP-ISSMP

Information Systems Security Management Professional

NEW QUESTION 1
Which of the following fields of management focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life?

A. Configuration management
B. Risk management
C. Procurement management
D. Change management

Answer: A

NEW QUESTION 2
Which of the following involves changing data prior to or during input to a computer in an effort to commit fraud?

A. Data diddling
B. Wiretapping
C. Eavesdropping
D. Spoofing

Answer: A

NEW QUESTION 3
Which of the following penetration testing phases involves reconnaissance or data gathering?

A. Attack phase
B. Pre-attack phase
C. Post-attack phase
D. Out-attack phase

Answer: B

NEW QUESTION 4
Which of the following protocols is used with a tunneling protocol to provide security?

A. FTP
B. IPX/SPX
C. IPSec
D. EAP

Answer: C

NEW QUESTION 5
Which of the following is the best method to stop vulnerability attacks on a Web server?

A. Using strong passwords
B. Configuring a firewall
C. Implementing the latest virus scanner
D. Installing service packs and updates

Answer: D

NEW QUESTION 6
Which of the following is NOT a valid maturity level of the Software Capability Maturity Model (CMM)?

A. Managed level
B. Defined level
C. Fundamental level
D. Repeatable level

Answer: C

NEW QUESTION 7
Which of the following BCP teams is the first responder and deals with the immediate effects of the disaster?

A. Emergency-management team
B. Damage-assessment team
C. Off-site storage team
D. Emergency action team

Answer: D

NEW QUESTION 8
Which of the following relies on a physical characteristic of the user to verify his identity?

A. Social Engineering
B. Kerberos v5
C. Biometrics
D. CHAP

Answer: C

NEW QUESTION 9
Which of the following statements about system hardening are true? Each correct answer represents a complete solution. Choose two.

A. It can be achieved by installing service packs and security updates on a regular basis.
B. It is used for securing the computer hardware.
C. It can be achieved by locking the computer room.
D. It is used for securing an operating syste

Answer: AD

NEW QUESTION 10
Which of the following processes is described in the statement below? "It is the process of implementing risk response plans, tracking identified risks, monitoring residual risk, identifying new risks, and evaluating risk process effectiveness throughout the project."

A. Monitor and Control Risks
B. Identify Risks
C. Perform Qualitative Risk Analysis
D. Perform Quantitative Risk Analysis

Answer: A

NEW QUESTION 10
Which of the following can be prevented by an organization using job rotation and separation of duties policies?

A. Collusion
B. Eavesdropping
C. Buffer overflow
D. Phishing

Answer: A

NEW QUESTION 14
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 17
What component of the change management system is responsible for evaluating, testing, and documenting changes created to the project scope?

A. Scope Verification
B. Project Management Information System
C. Integrated Change Control
D. Configuration Management System

Answer: D

NEW QUESTION 22
Electronic communication technology refers to technology devices, such as computers and cell phones, used to facilitate communication. Which of the following is/are a type of electronic communication? Each correct answer represents a complete solution. Choose all that apply.

A. Internet telephony
B. Instant messaging
C. Electronic mail
D. Post-it note
E. Blogs
F. Internet teleconferencing

Answer: ABCEF

NEW QUESTION 27
Which of the following statements about the integrity concept of information security management are true? Each correct answer represents a complete solution. Choose three.

A. It ensures that unauthorized modifications are not made to data by authorized personnel orprocesses.
B. It determines the actions and behaviors of a single individual within a system
C. It ensures that modifications are not made to data by unauthorized personnel or processes.
D. It ensures that internal information is consistent among all subentities and also consistent with the real-world, external situation.

Answer: ACD

NEW QUESTION 31
Which of the following contract types is described in the statement below? "This contract type provides no incentive for the contractor to control costs and hence is rarely utilized."

A. Cost Plus Fixed Fee
B. Cost Plus Percentage of Cost
C. Cost Plus Incentive Fee
D. Cost Plus Award Fee

Answer: B

NEW QUESTION 34
Ned is the program manager for his organization and he's considering some new materials for his program. He and his team have never worked with these materials before and he wants to ask the vendor for some additional information, a demon, and even some samples. What type of a document should Ned send to the vendor?

A. IFB
B. RFQ
C. RFP
D. RFI

Answer: D

NEW QUESTION 38
Against which of the following does SSH provide protection? Each correct answer represents a complete solution. Choose two.

A. IP spoofing
B. Broadcast storm
C. Password sniffing
D. DoS attack

Answer: AC

NEW QUESTION 39
Which of the following roles is responsible for review and risk analysis of all contracts on a regular basis?

A. The Configuration Manager
B. The Supplier Manager
C. The Service Catalogue Manager
D. The IT Service Continuity Manager

Answer: B

NEW QUESTION 41
Which of the following laws or acts, formed in Australia, enforces prohibition against cyber stalking?

A. Malicious Communications Act (1998)
B. Anti-Cyber-Stalking law (1999)
C. Stalking Amendment Act(1999)
D. Stalking by Electronic Communications Act (2001)

Answer: C

NEW QUESTION 45
Mark works as a security manager for SofTech Inc. He is working in a partially equipped office space which contains some of the system hardware, software, telecommunications, and power sources. In which of the following types of office sites is he working?

A. Mobile site
B. Warm site
C. Cold site
D. Hot site

Answer: B

NEW QUESTION 48
Which of the following are the major tasks of risk management? Each correct answer represents a complete solution. Choose two.

A. Assuring the integrity of organizational data

B. Building Risk free systems
C. Risk control
D. Risk identification

Answer: CD

NEW QUESTION 50
Which of the following statements about Due Care policy is true?

A. It is a method used to authenticate users on a network.
B. It is a method for securing database servers.
C. It identifies the level of confidentiality of information.
D. It provides information about new viruse

Answer: C

NEW QUESTION 55
What are the steps related to the vulnerability management program? Each correct answer represents a complete solution. Choose all that apply.

A. Maintain and Monitor
B. Organization Vulnerability
C. Define Policy
D. Baseline the Environment

Answer: ACD

NEW QUESTION 59
Which of the following sections come under the ISO/IEC 27002 standard?

A. Financial assessment
B. Asset management
C. Security policy
D. Risk assessment

Answer: BCD

NEW QUESTION 62
Which of the following access control models uses a predefined set of access privileges for an object of a system?

A. Role-Based Access Control
B. Mandatory Access Control
C. Policy Access Control
D. Discretionary Access Control

Answer: B

NEW QUESTION 65
Which of the following needs to be documented to preserve evidences for presentation in court?

A. Separation of duties
B. Account lockout policy
C. Incident response policy
D. Chain of custody

Answer: D

NEW QUESTION 67
Which of the following statements best explains how encryption works on the Internet?

A. Encryption encodes information using specific algorithms with a string of numbers known as a key.
B. Encryption validates a username and passwordbefore sending information to the Web server.
C. Encryption allows authorized users to access Web sites that offer online shopping.
D. Encryption helps in transaction processing by e-commerce servers on the Interne

Answer: A

NEW QUESTION 70
Which of the following statutes is enacted in the U.S., which prohibits creditors from collecting data from applicants, such as national origin, caste, religion etc?

A. The Fair Credit Reporting Act (FCRA)
B. The Privacy Act
C. The Electronic Communications Privacy Act
D. The Equal Credit Opportunity Act (ECOA)

Answer: D

NEW QUESTION 73
Which of the following security models focuses on data confidentiality and controlled access to classified information?

A. Bell-La Padula model
B. Take-Grant model
C. Clark-Wilson model
D. Biba model

Answer: A

NEW QUESTION 77
Which of the following recovery plans includes specific strategies and actions to deal with specific variances to assumptions resulting in a particular security problem, emergency, or state of affairs?

A. Disaster recovery plan
B. Contingency plan
C. Continuity of Operations Plan
D. Business continuity plan

Answer: B

NEW QUESTION 78
Which of the following BCP teams handles financial arrangement, public relations, and media inquiries in the time of disaster recovery?

A. Software team
B. Off-site storage team
C. Applications team
D. Emergency-management team

Answer: D

NEW QUESTION 83
Eric is the project manager of the NQQ Project and has hired the ZAS Corporation to complete part of the project work for Eric's organization. Due to a change request the ZAS Corporation is no longer needed on the project even though they have completed nearly all of the project work. Is Eric's organization liable to pay the ZAS Corporation for the work they have completed so far on the project?

A. Yes, the ZAS Corporation did not choose to terminate the contract work.
B. It depends on what the outcome of a lawsuit will determine.
C. It dependson what the termination clause of the contract stipulates.
D. No, the ZAS Corporation did not complete all of the wor

Answer: C

NEW QUESTION 88
Della works as a security manager for SoftTech Inc. She is training some of the newly recruited personnel in the field of security management. She is giving a tutorial on DRP. She explains that the major goal of a disaster recovery plan is to provide an organized way to make decisions if a disruptive event occurs and asks for the other objectives of the DRP. If you are among some of the newly recruited personnel in SoftTech Inc, what will be your answer for her question? Each correct answer represents a part of the solution. Choose three.

A. Protect an organization from major computer services failure.
B. Minimizethe risk to the organization from delays in providing services.
C. Guarantee the reliability of standby systems through testing and simulation.
D. Maximize the decision-making required by personnel during a disaste

Answer: ABC

NEW QUESTION 93
Software Development Life Cycle (SDLC) is a logical process used by programmers to develop software. Which of the following SDLC phases meets the audit objectives defined below: System and data are validated. System meets all user requirements. System meets all control requirements.

A. Programming and training
B. Evaluation and acceptance
C. Definition
D. Initiation

Answer: B

NEW QUESTION 94
Which of the following are the examples of administrative controls? Each correct answer represents a complete solution. Choose all that apply.

A. Security awareness training
B. Security policy
C. Data Backup
D. Auditing

Answer:

AB

NEW QUESTION 97
Which of the following are the types of access controls? Each correct answer represents a complete solution. Choose three.

A. Administrative
B. Automatic
C. Physical
D. Technical

Answer: ACD

NEW QUESTION 99
Which of the following representatives of incident response team takes forensic backups of the systems that are the focus of the incident?

A. Legalrepresentative
B. Technical representative
C. Lead investigator
D. Information security representative

Answer: B

NEW QUESTION 100
Which of the following persons is responsible for testing and verifying whether the security policy is properly implemented, and the derived security solutions are adequate or not?

A. Data custodian
B. Auditor
C. User
D. Data owner

Answer: B

NEW QUESTION 103
You work as the Network Administrator for a defense contractor. Your company works with sensitive materials and all IT personnel have at least a secret level clearance. You are still concerned that one individual could perhaps compromise the network (intentionally or unintentionally) by setting up improper or unauthorized remote access. What is the best way to avoid this problem?

A. Implement separation of duties.
B. Implement RBAC.
C. Implement three way authentication.
D. Implement least privilege

Answer: A

NEW QUESTION 108
Mark works as a security manager for SoftTech Inc. He is performing a security awareness program. To be successful in performing the awareness program, he should take into account the needs and current levels of training and understanding of the employees and audience. There are
five key ways, which Mark should keep in mind while performing this activity. Current level of computer usage What the audience really wants to learn How receptive the audience is to the security program How to gain acceptance Who might be a possible ally Which of the following activities is performed in this security awareness process?

A. Separation of duties
B. Stunned owl syndrome
C. Audience participation
D. Audience segmentation

Answer: D

NEW QUESTION 112
In which of the following phases of the SDLC does the software and other components of the system faithfully incorporate the design specifications and provide proper documentation and training?

A. Programming andtraining
B. Evaluation and acceptance
C. Initiation
D. Design

Answer: A

NEW QUESTION 117
Which of the following signatures watches for the connection attempts to well-known, frequently attacked ports?

A. Port signatures
B. Digital signatures
C. Header condition signatures

D. String signatures

Answer: A

NEW QUESTION 120
Configuration Management (CM) is an Information Technology Infrastructure Library (ITIL) IT
Service Management (ITSM) process. Configuration Management is used for which of the following? 1.To account for all IT assets 2.To provide precise information support to other ITIL disciplines 3.To provide a solid base only for Incident and Problem Management 4.To verify configuration records and correct any exceptions

A. 1, 3, and 4 only
B. 2 and 4 only
C. 1, 2, and 4 only
D. 2, 3, and 4 only

Answer: C

NEW QUESTION 124
Which of the following rate systems of the Orange book has no security controls?

A. D-rated
B. C-rated
C. E-rated
D. A-rated

Answer: A

NEW QUESTION 129
Which of the following documents is described in the statement below? "It is developed along with all processes of the risk management. It contains the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning."

A. Risk register
B. Risk management plan
C. Quality management plan
D. Project charter

Answer: A

NEW QUESTION 134
Which of the following test methods has the objective to test the IT system from the viewpoint of a threat- source and to identify potential failures in the IT system protection schemes?

A. Penetration testing
B. On-site interviews
C. Security Test and Evaluation (ST&E)
D. Automated vulnerability scanning tool

Answer: A

NEW QUESTION 135
Which of the following statements reflect the 'Code of Ethics Preamble' in the '(ISC)2 Code of Ethics'? Each correct answer represents a complete solution. Choose all that apply.

A. Strict adherence to this Code is a condition of certification.
B. Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
C. Advance and protect the profession.
D. Provide diligent and competent service to principal

Answer: AB

NEW QUESTION 138
Which of the following options is an approach to restricting system access to authorized users?

A. DAC
B. MIC
C. RBAC
D. MAC

Answer: C

NEW QUESTION 140
You are the project manager for TTX project. You have to procure some electronics gadgets for the project. A relative of yours is in the retail business of those gadgets. He approaches you for your favor to get the order. This is the situation of .

A. Conflict of interest
B. Bribery
C. Illegal practice
D. Irresponsible practice

Answer: A

NEW QUESTION 142
What course of action can be taken by a party if the current negotiations fail and an agreement cannot be reached?

A. ZOPA
B. PON
C. Bias
D. BATNA

Answer: D

NEW QUESTION 147
Which of the following is a documentation of guidelines that computer forensics experts use to handle evidences?

A. Evidence access policy
B. Incident responsepolicy
C. Chain of custody
D. Chain of evidence

Answer: C

NEW QUESTION 151
Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?

A. Safeguard
B. Single Loss Expectancy (SLE)
C. Exposure Factor (EF)
D. Annualized Rate of Occurrence (ARO)

Answer: D

NEW QUESTION 153
Which of the following statements is related with the second law of OPSEC?

A. If you are not protecting it (the critical and sensitive information), the adversary wins!
B. If you don't know what to protect, how do you know you are protecting it?
C. If you don't know about your security resources you could not protect your network.
D. If you don't know the threat, how do you know what to protect?

Answer: B

NEW QUESTION 156
Fill in the blank with an appropriate phrase. An is an intensive application of the OPSEC process to an existing operation or activity by a multidiscipline team of experts.

A. OPSEC assessment

Answer: A

NEW QUESTION 159
Which of the following are the levels of public or commercial data classification system? Each correct answer represents a complete solution. Choose all that apply.

A. Secret
B. Sensitive
C. Unclassified
D. Private
E. Confidential
F. Public

Answer: BDEF

NEW QUESTION 160
Which of the following is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known, but by which a business can obtain an economic advantage over its competitors?

A. Utility model
B. Cookie
C. Copyright

D. Trade secret

Answer: D

NEW QUESTION 162
Which of the following backup sites takes the longest recovery time?

A. Cold site
B. Hot site
C. Warm site
D. Mobile backup site

Answer: A

NEW QUESTION 163
Which of the following is the default port for Simple Network Management Protocol (SNMP)?

A. TCP port 80
B. TCP port 25
C. UDP port 161
D. TCP port 110

Answer: C

NEW QUESTION 165
Which of the following statements about Hypertext Transfer Protocol Secure (HTTPS) are true? Each correct answer represents a complete solution. Choose two.

A. It uses TCP port 80 as the default port.
B. It is a protocol used in the Universal Resource Locater (URL) address line to connect to a secure site.
C. It uses TCP port 443 as the default port.
D. It is a protocol used to provide security for a database server in an internal networ

Answer: BC

NEW QUESTION 167
NIST Special Publication 800-50 is a security awareness program. It is designed for those people who are currently working in the information technology field and want information on security policies. Which of the following are some of its critical steps? Each correct answer represents a complete solution. Choose two.

A. Awareness and Training Material Effectiveness
B. Awareness and Training Material Development
C. Awareness and Training Material Implementation
D. Awareness and Training Program Design

Answer: BD

NEW QUESTION 171
You are the program manager for your project. You are working with the project managers regarding the procurement processes for their projects. You have ruled out one particular contract type because it is considered too risky for the program. Which one of the following contract types is usually considered to be the most dangerous for the buyer?

A. Cost plus incentive fee
B. Fixed fee
C. Cost plus percentage of costs
D. Time and materials

Answer: C

NEW QUESTION 173
In which of the following contract types, the seller is reimbursed for all allowable costs for performing the contract work and receives a fixed fee payment which is calculated as a percentage of the initial estimated project costs?

A. Firm Fixed Price Contracts
B. Cost Plus Fixed Fee Contracts
C. Fixed Price Incentive Fee Contracts
D. Cost Plus Incentive Fee Contracts

Answer: B

NEW QUESTION 177
Which of the following processes is a structured approach to transitioning individuals, teams, and organizations from a current state to a desired future state?

A. Risk management
B. Configuration management
C. Change management
D. Procurement management

Answer: C

NEW QUESTION 179
DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. What phases are identified by DIACAP? Each correct answer represents a complete solution. Choose all that apply.

A. System Definition
B. Accreditation
C. Verification
D. Re-Accreditation
E. Validation
F. Identification

Answer: ACDE

NEW QUESTION 181
Management has asked you to perform a risk audit and report back on the results. Bonny, a project team member asks you what a risk audit is. What do you tell Bonny?

A. A risk audit is a review of all the risks that have yet to occur and what their probability of happening are.
B. A risk audit is a review of the effectiveness of the risk responses in dealing with identified risks and their root causes, as well as the effectiveness of the risk management process.
C. A risk audit is a review of all the risk probability and impact for the risks, which are still present in the project but which have not yet occurred.
D. A risk audit is an audit of all the risks that have occurred in the project and what their true impact on cost and time has been.

Answer: B

NEW QUESTION 182
You work as a security manager for SoftTech Inc. You are conducting a security awareness campaign for your employees. Which of the following ideas will you consider the best when
conducting a security awareness campaign?

A. Target system administrators and the help desk.
B. Provide technical details on exploits.
C. Provide customizedmessages for different groups.
D. Target senior managers and business process owner

Answer: C

NEW QUESTION 187
Which of the following SDLC phases consists of the given security controls. Misuse Case Modeling Security Design and Architecture Review Threat and Risk Modeling Security Requirements and Test Cases Generation

A. Design
B. Maintenance
C. Deployment
D. Requirements Gathering

Answer: A

NEW QUESTION 191
Which of the following liabilities is a third-party liability in which an individual may be responsible for an action by another party?

A. Relational liability
B. Engaged liability
C. Contributory liability
D. Vicarious liability

Answer: D

NEW QUESTION 193
Which of the following measurements of an enterprise's security state is the process whereby an organization establishes the parameters within which programs, investments, and acquisitions reach the desired results?

A. Information sharing
B. Ethics
C. Performance measurement
D. Risk management

Answer: C

NEW QUESTION 198
Tomas is the project manager of the QWS Project and is worried that the project stakeholders will want to change the project scope frequently. His fear is based on the many open issues in the project and how the resolution of the issues may lead to additional project changes. On what document are Tomas and the

stakeholders working in this scenario?

A. Communications management plan
B. Change management plan
C. Issue log
D. Risk management plan

Answer: B

NEW QUESTION 200
Fill in the blank with an appropriate word. are used in information security to formalize security policies.

A. Model

Answer: A

NEW QUESTION 202
Which of the following are known as the three laws of OPSEC? Each correct answer represents a part of the solution. Choose three.

A. Ifyou don't know the threat, how do you know what to protect?
B. If you don't know what to protect, how do you know you are protecting it?
C. If you are not protecting it (the critical and sensitive information), the adversary wins!
D. If you don't knowabout your security resources you cannot protect your networ

Answer: ABC

NEW QUESTION 206
In which of the following alternative processing sites is the backup facility maintained in a constant order, with a full complement of servers, workstations, and communication links ready to assume the primary operations responsibility?

A. Mobile Site
B. Cold Site
C. Warm Site
D. Hot Site

Answer: D

NEW QUESTION 210
Which of the following processes is used by remote users to make a secure connection to internal resources after establishing an Internet connection?

A. Packet filtering
B. Tunneling
C. Packet sniffing
D. Spoofing

Answer: B

NEW QUESTION 215
Which of the following is a name, symbol, or slogan with which a product is identified?

A. Copyright
B. Trademark
C. Trade secret
D. Patent

Answer: B

NEW QUESTION 220
Which of the following concepts represent the three fundamental principles of information security? Each correct answer represents a complete solution. Choose three.

A. Confidentiality
B. Integrity
C. Availability
D. Privacy

Answer: ABC

NEW QUESTION 224
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CISSP-ISSMP Practice Exam Features:

* CISSP-ISSMP Questions and Answers Updated Frequently

* CISSP-ISSMP Practice Questions Verified by Expert Senior Certified Staff

* CISSP-ISSMP Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CISSP-ISSMP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year