

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 are the ways of sending secure e-mail messages over the Internet? Each correct answer represents a complete solution. Choose two.

- A. TLS
- B. PGP
- C. S/MIME
- D. IPSec

Answer: BC

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

Mark works as a security manager for SoftTech Inc. He is involved in the BIA phase to create a document to be used to help understand what impact a disruptive event would have on the business. The impact might be financial or operational. Which of the following are the objectives related to the above phase in which Mark is involved? Each correct answer represents a part of the solution. Choose three.

- A. Resource requirements identification
- B. Criticality prioritization
- C. Down-time estimation
- D. Performing vulnerability assessment

Answer: ABC

NEW QUESTION 5

Which of the following characteristics are described by the DIAP Information Readiness Assessment function? Each correct answer represents a complete solution. Choose all that apply.

- A. It performs vulnerability/threat analysis assessment.
- B. It identifies and generates IA requirements.
- C. It provides data needed to accurately assess IA readiness.
- D. It provides for entry and storage of individual system data

Answer: ABC

NEW QUESTION 6

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 7

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 8

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 9

You work as a Network Administrator for ABC Inc. The company uses a secure wireless network. John complains to you that his computer is not working properly. What type of security audit do you need to conduct to resolve the problem?

- A. Operational audit
- B. Dependent audit
- C. Non-operational audit
- D. Independent audit

Answer: D

NEW QUESTION 10

Which of the following are the common roles with regard to data in an information classification program? Each correct answer represents a complete solution. Choose all that apply.

- A. Editor
- B. Custodian
- C. Owner
- D. Security auditor
- E. User

Answer: BCDE

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 15

Walter is the project manager of a large construction project. He'll be working with several vendors on the project. Vendors will be providing materials and labor for several parts of the project. Some of the works in the project are very dangerous so Walter has implemented safety requirements for all of the vendors and his own project team. Stakeholders for the project have added new requirements, which have caused new risks in the project. A vendor has identified a new risk that could affect the project if it comes into fruition. Walter agrees with the vendor and has updated the risk register and created potential risk responses to mitigate the risk. What should Walter also update in this scenario considering the risk event?

- A. Project contractual relationship with the vendor
- B. Project management plan
- C. Project communications plan
- D. Project scope statement

Answer: B

NEW QUESTION 18

You are the project manager of the HJK Project for your organization. You and the project team have created risk responses for many of the risk events in the project. Where should you document the proposed responses and the current status of all identified risks?

- A. Risk management plan
- B. Lessons learned documentation
- C. Risk register
- D. Stakeholder management strategy

Answer: C

NEW QUESTION 23

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 27

Which of the following analysis provides a foundation for measuring investment of time, money and human resources required to achieve a particular outcome?

- A. Vulnerability analysis
- B. Cost-benefit analysis
- C. Gap analysis
- D. Requirement analysis

Answer: C

NEW QUESTION 32

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: B

NEW QUESTION 34

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 36

Which of the following acts is a specialized privacy bill that affects any educational institution to accept any form of funding from the federal government?

- A. HIPAA
- B. COPPA
- C. FERPA
- D. GLBA

Answer: C

NEW QUESTION 39

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 or processes.
- 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 43

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 demo, 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 46

You are a project manager of a large construction project. Within the project you are working with several vendors to complete different phases of the construction. Your client has asked that you arrange for some of the materials a vendor is to install next week in the project to be changed. According to the change management plan what subsystem will need to manage this change request?

- A. Cost
- B. Resources
- C. Contract
- D. Schedule

Answer: C

NEW QUESTION 49

In which of the following SDLC phases is the system's security features configured and enabled, the system is tested and installed or fielded, and the system is authorized for processing?

- A. Initiation Phase
- B. Development/Acquisition Phase
- C. Implementation Phase
- D. Operation/Maintenance Phase

Answer: C

NEW QUESTION 54

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 58

Which of the following response teams aims to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large?

- A. CSIRT
- B. CERT
- C. FIRST
- D. FedCIRC

Answer: C

NEW QUESTION 60

Which of the following statements is related with the first 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: D

NEW QUESTION 63

Which of the following evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person?

- A. Direct
- B. Circumstantial
- C. Incontrovertible
- D. Corroborating

Answer: B

NEW QUESTION 67

Which of the following Acts enacted in United States amends Civil Rights Act of 1964, providing technical changes affecting the length of time allowed to challenge unlawful seniority provisions, to sue the federal government for discrimination and to bring age discrimination claims?

- A. PROTECT Act
- B. Sexual Predators Act
- C. Civil Rights Act of 1991
- D. The USA Patriot Act of 2001

Answer: C

NEW QUESTION 71

Which of the following policies helps reduce the potential damage from the actions of one person?

- A. CSA
- B. Risk assessment
- C. Separation of duties
- D. Internal audit

Answer: C

NEW QUESTION 73

The goal of Change Management is to ensure that standardized methods and procedures are used for efficient handling of all changes. Which of the following are Change Management terminologies? Each correct answer represents a part of the solution. Choose three.

- A. Request for Change
- B. Service Request Management
- C. Change
- D. Forward Schedule of Changes

Answer: ACD

NEW QUESTION 75

Which of the following is the correct order of digital investigations Standard Operating Procedure (SOP)?

- A. Initial analysis, request for service, data collection, data reporting, data analysis
- B. Initial analysis, request for service, data collection, data analysis, data reporting
- C. Request for service, initial analysis, data collection, data analysis, data reporting
- D. Request for service, initial analysis, data collection, data reporting, data analysis

Answer: C

NEW QUESTION 80

Which of the following roles is used to ensure that the confidentiality, integrity, and availability of the services are maintained to the levels approved on the Service Level Agreement (SLA)?

- A. The Service Level Manager
- B. The Configuration Manager
- C. The IT Security Manager
- D. The Change Manager

Answer: C

NEW QUESTION 84

Which of the following is a process of monitoring data packets that travel across a network?

- A. Password guessing
- B. Packet sniffing
- C. Shielding
- D. Packet filtering

Answer: B

NEW QUESTION 88

You are documenting your organization's change control procedures for project management. What portion of the change control process oversees features and functions of the product scope?

- A. Configuration management
- B. Product scope management is outside the concerns of the project.
- C. Scope changecontrol system
- D. Project integration management

Answer: A

NEW QUESTION 89

Which of the following statements best describes the consequences of the disaster recovery plan test?

- A. If no deficiencies were found during the test, then the test was probably flawed.
- B. The plan should not be changed no matter what the results of the test would be.
- C. The results of the test should be kept secret.
- D. If no deficiencies were found during the test, then the plan is probably perfec

Answer: A

NEW QUESTION 90

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 94

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 99

Which of the following is a documentation of guidelines that are used to create archival copies of important data?

- A. User policy
- B. Security policy
- C. Audit policy
- D. Backup policy

Answer: D

NEW QUESTION 100

Which of the following deals is a binding agreement between two or more persons that is enforceable by law?

- A. Outsource
- B. Proposal
- C. Contract
- D. Service level agreement

Answer: C

NEW QUESTION 105

Which of the following types of agreement creates a confidential relationship between the parties to protect any type of confidential and proprietary information or a trade secret?

- A. SLA
- B. NDA
- C. Non-price competition
- D. CNC

Answer: B

NEW QUESTION 110

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 112

Which of the following U.S. Federal laws addresses computer crime activities in communication lines, stations, or systems?

- A. 18 U.S.
- B. 1362
- C. 18 U.S.
- D. 1030
- E. 18 U.S.
- F. 1029
- G. 18 U.S.
- H. 2701
- I. 18 U.S.
- J. 2510

Answer: A

NEW QUESTION 116

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 118

Which of the following is a process that identifies critical information to determine if friendly actions can be observed by adversary intelligence systems?

- A. IDS
- B. OPSEC
- C. HIDS
- D. NIDS

Answer: B

NEW QUESTION 122

Which of the following processes will you involve to perform the active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures?

- A. Penetration testing
- B. Risk analysis
- C. Baselineing
- D. Compliance checking

Answer: A

NEW QUESTION 127

Which of the following are the levels of military data classification system? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABCDE

NEW QUESTION 132

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 137

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 141

Fill in the blank with an appropriate phrase. is the process of using a strategy and plan of what patches should be applied to which systems at a specified time.
Correct

- A. Patch management

Answer: A

NEW QUESTION 143

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 148

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 151

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. Qualitative risk analysis
- C. Requested changes
- D. Risk audits

Answer: C

NEW QUESTION 155

You are the project manager of the NGQQ Project for your company. To help you communicate project status to your stakeholders, you are going to create a stakeholder register. All of the following information should be included in the stakeholder register except for which one?

- A. Identification information for each stakeholder
- B. Assessment information of the stakeholders' major requirements, expectations, and potential influence
- C. Stakeholder classification of their role in the project
- D. Stakeholder management strategy

Answer: D

NEW QUESTION 160

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 162

Which of the following laws enacted in United States makes it illegal for an Internet Service Provider (ISP) to allow child pornography to exist on Web sites?

- A. Child Pornography Prevention Act (CPPA)
- B. USA PATRIOT Act
- C. Prosecutorial Remedies and Tools Against the Exploitation of Children Today Act (PROTECT Act)
- D. Sexual Predators Act

Answer: D

NEW QUESTION 165

Which of the following statements are true about security risks? Each correct answer represents a complete solution. Choose three.

- A. They can be analyzed and measured by the risk analysis process.
- B. They can be removed completely by taking proper actions.
- C. They can be mitigated by reviewing and taking responsible actions based on possible risks.
- D. They are considered an indicator of threats coupled with vulnerabilit

Answer: ACD

NEW QUESTION 166

Which of the following architecturally related vulnerabilities is a hardware or software mechanism, which was installed to permit system maintenance and to bypass the system's security protections?

- A. Maintenance hook
- B. Lack of parameter checking
- C. Time of Check to Time of Use (TOC/TOU) attack
- D. Covert channel

Answer: A

NEW QUESTION 169

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

Answer: B

NEW QUESTION 174

Which of the following are the process steps of OPSEC? Each correct answer represents a part of the solution. Choose all that apply.

- A. Analysis of Vulnerabilities
- B. Display of associated vulnerability components
- C. Assessment of Risk
- D. Identification of Critical Information

Answer: ACD

NEW QUESTION 176

You work as a project manager for SoftTech Inc. A threat with a dollar value of \$150,000 is expected to happen in your project and the frequency of threat occurrence per year is 0.001. What will be the annualized loss expectancy in your project?

- A. \$180.25
- B. \$150
- C. \$100
- D. \$120

Answer: B

NEW QUESTION 177

Which of the following are the responsibilities of the owner with regard to data in an information classification program? Each correct answer represents a complete solution. Choose three.

- A. Determining what level of classification the information requires.
- B. Delegating the responsibility of the data protection duties to a custodian.
- C. Reviewing the classification assignments at regular time intervals and making changes as the business needs change.
- D. Running regular backups and routinely testing the validity of the backup dat

Answer: ABC

NEW QUESTION 179

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 184

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 186

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 187

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 188

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 189

Which of the following terms describes a repudiation of a contract that occurs before the time when performance is due?

- A. Expected breach
- B. Actual breach
- C. Anticipatory breach
- D. Nonperforming breach

Answer: C

NEW QUESTION 190

Which of the following is generally practiced by the police or any other recognized governmental authority?

- A. Phishing
- B. Wiretapping
- C. SMB signing
- D. Spoofing

Answer: B

NEW QUESTION 193

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 197

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 201

You company suspects an employee of sending unauthorized emails to competitors. These emails are alleged to contain confidential company data. Which of the following is the most important step for you to take in preserving the chain of custody?

- A. Preserve the email server including all logs.
- B. Seize the employee's PC.
- C. Make copies of that employee's email.
- D. Place spyware on the employee's PC to confirm these activities

Answer: A

NEW QUESTION 203

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 204

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 209

The incident response team has turned the evidence over to the forensic team. Now, it is the time to begin looking for the ways to improve the incident response process for next time. What are the typical areas for improvement? Each correct answer represents a complete solution. Choose all that apply.

- A. Information dissemination policy
- B. Electronic monitoring statement
- C. Additional personnel security controls
- D. Incident response plan

Answer: ABCD

NEW QUESTION 210

Which of the following attacks can be mitigated by providing proper training to the employees in an organization?

- A. Social engineering
- B. Smurf
- C. Denial-of-Service
- D. Man-in-the-middle

Answer: A

NEW QUESTION 215

You work as a Forensic Investigator. Which of the following rules will you follow while working on a case? Each correct answer represents a part of the solution. Choose all that apply.

- A. Prepare a chain of custody and handle the evidence carefully.
- B. Examine original evidence and never rely on the duplicate evidence.
- C. Never exceed the knowledge base of the forensic investigation.
- D. Follow the rules of evidence and never temper with the evidence.

Answer: ABCD

NEW QUESTION 218

You are the Network Administrator for a college. You watch a large number of people (some not even students) going in and out of areas with campus computers (libraries, computer labs, etc.). You have had a problem with laptops being stolen. What is the most cost effective method to prevent this?

- A. Videosurveillance on all areas with computers.
- B. Use laptop locks.
- C. Appoint a security guard.
- D. Smart card access to all areas with computers.

Answer: B

NEW QUESTION 222

Shoulder surfing is a type of in-person attack in which the attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard of an employee's computer while he is typing in his password at any access point such as a terminal/Web site. Which of the following is violated in a shoulder surfing attack?

- A. Availability
- B. Confidentiality
- C. Integrity
- D. Authenticity

Answer: B

NEW QUESTION 224

Which of the following plans provides procedures for recovering business operations immediately following a disaster?

- A. Disaster recovery plan

- B. Business continuity plan
- C. Continuity of operation plan
- D. Business recovery plan

Answer: D

NEW QUESTION 227

Mark is the project manager of the NHQ project in Spartech Inc. The project has an asset valued at \$195,000 and is subjected to an exposure factor of 35 percent. What will be the Single Loss Expectancy of the project?

- A. \$92,600
- B. \$67,250
- C. \$68,250
- D. \$72,650

Answer: C

NEW QUESTION 229

Which of the following steps are generally followed in computer forensic examinations? Each correct answer represents a complete solution. Choose three.

- A. Acquire
- B. Analyze
- C. Authenticate
- D. Encrypt

Answer: ABC

NEW QUESTION 231

Which of the following 'Code of Ethics Canons' of the '(ISC)2 Code of Ethics' states to act honorably, honestly, justly, responsibly and legally?

- A. Second Code of Ethics Canons
- B. Fourth Code of Ethics Canons
- C. First Code of Ethics Canons
- D. Third Code of Ethics Canons

Answer: A

NEW QUESTION 236

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 238

You are the Network Administrator for a software company. Due to the nature of your company's business, you have a significant number of highly computer savvy users. However, you have still decided to limit each user access to only those resources required for their job, rather than give wider access to the technical users (such as tech support and software engineering personnel).

What is this an example of?

- A. The principle of maximum control.
- B. The principle of least privileges.
- C. Proper use of an ACL.
- D. Poor resource managemen

Answer: B

NEW QUESTION 240

Which of the following are examples of administrative controls that involve all levels of employees within an organization and determine which users have access to what resources and information? Each correct answer represents a complete solution. Choose three.

- A. Employee registration and accounting
- B. Disaster preparedness and recovery plans
- C. Network authentication
- D. Training and awareness
- E. Encryption

Answer: ABD

NEW QUESTION 242

Which of the following divisions of the Trusted Computer System Evaluation Criteria (TCSEC) is based on the Mandatory Access Control (MAC) policy?

- A. Division A
- B. Division D
- C. Division B
- D. Division C

Answer: C

NEW QUESTION 246

Which of the following sites are similar to the hot site facilities, with the exception that they are completely dedicated, self-developed recovery facilities?

- A. Cold sites
- B. Orange sites
- C. Warm sites
- D. Duplicate processing facilities

Answer: D

NEW QUESTION 247

Which of the following plans is documented and organized for emergency response, backup operations, and recovery maintained by an activity as part of its security program that will ensure the availability of critical resources and facilitates the continuity of operations in an emergency situation?

- A. Disaster Recovery Plan
- B. Contingency Plan
- C. Continuity Of Operations Plan
- D. Business Continuity Plan

Answer: B

NEW QUESTION 252

Which of the following laws is defined as the Law of Nations or the legal norms that has developed through the customary exchanges between states over time, whether based on diplomacy or aggression?

- A. Customary
- B. Tort
- C. Criminal
- D. Administrative

Answer: A

NEW QUESTION 257

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 262

Sarah has created a site on which she publishes a copyrighted material. She is ignorant that she is infringing copyright. Is she guilty under copyright laws?

- A. No
- B. Yes

Answer: B

NEW QUESTION 263

You work as the Senior Project manager in Dotcoiss Inc. Your company has started a software project using configuration management and has completed 70% of it. You need to ensure that the network infrastructure devices and networking standards used in this project are installed in accordance with the requirements of its detailed project design documentation. Which of the following procedures will you employ to accomplish the task?

- A. Configuration identification
- B. Physical configuration audit
- C. Configuration control
- D. Functional configuration audit

Answer: B

NEW QUESTION 265

Which of the following access control models are used in the commercial sector? Each correct answer represents a complete solution. Choose two.

- A. Clark-Biba model
- B. Clark-Wilson model
- C. Bell-LaPadula model

D. Biba model

Answer: BD

NEW QUESTION 268

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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

100% Actual & Verified — Instant Download, Please Click
[Order The CISSP-ISSMP Practice Test Here](#)