



ISC2

Exam Questions 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 is the process performed between organizations that have unique hardware or software that cannot be maintained at a hot or warm site?

- A. Cold sites arrangement
- B. Business impact analysis
- C. Duplicate processing facilities
- D. Reciprocal agreements

Answer: D

NEW QUESTION 4

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 5

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 6

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 dat

Answer: ABC

NEW QUESTION 7

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 8

Which of the following security models dictates that subjects can only access objects through applications?

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

Answer: C

NEW QUESTION 9

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 10

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

Answer: B

NEW QUESTION 10

You are the project manager of the GHE Project. You have identified the following risks with the characteristics as shown in the following figure:

Risk	Probability	Impact
A	.60	-10,000
B	.10	-85,000
C	.25	-75,000
D	.40	45,000
E	.50	-17,000

How much capital should the project set aside for the risk contingency reserve?

- A. \$142,000
- B. \$232,000
- C. \$41,750
- D. \$23,750

Answer: D

NEW QUESTION 11

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 system

Answer: AD

NEW QUESTION 15

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 16

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 21

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 24

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. Vulnerability Assessment and Penetration Testing
- B. Security Certification and Accreditation (C&A)
- C. Change and Configuration Control
- D. Risk Adjustments

Answer: ABD

NEW QUESTION 27

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 30

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 31

A contract cannot have provisions for which one of the following?

- A. Subcontracting the work
- B. Penalties and fines for disclosure of intellectual rights
- C. A deadline for the completion of the work
- D. Illegal activities

Answer: D

NEW QUESTION 33

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

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. A teaming agreement is an example of what risk response?

- A. Mitigation
- B. Sharing
- C. Acceptance
- D. Transference

Answer: B

NEW QUESTION 35

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 37

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

What is a stakeholder analysis chart?

- A. It is a matrix that documents stakeholders' threats, perceived threats, and communication needs.
- B. It is a matrix that identifies all of the stakeholders and to whom they must report to.
- C. It is a matrix that documents the stakeholders' requirements, when the requirements were created, and when the fulfillment of the requirements took place..
- D. It is a matrix that identifies who must communicate with who

Answer: A

NEW QUESTION 43

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 46

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 51

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 56

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 57

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 60

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 63

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 68

You are advising a school district on disaster recovery plans. In case a disaster affects the main IT centers for the district they will need to be able to work from an alternate location. However, budget is an issue. Which of the following is most appropriate for this client?

- A. Cold site
- B. Off site
- C. Hot site
- D. Warm site

Answer: A

NEW QUESTION 69

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 71

Which of the following issues are addressed by the change control phase in the maintenance phase of the life cycle models? Each correct answer represents a complete solution. Choose all that apply.

- A. Performing quality control
- B. Recreating and analyzing the problem
- C. Developing the changes and corresponding tests
- D. Establishing the priorities of requests

Answer: ABC

NEW QUESTION 75

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 viruses

Answer: C

NEW QUESTION 77

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

Answer: B

NEW QUESTION 81

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 85

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 87

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 92

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 93

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 98

Which of the following statements about the availability concept of Information security management is true?

- A. It determines actions and behaviors of a single individual within a system.
- B. It ensures reliable and timely access to resources.
- C. It ensures that unauthorized modifications are not made to data by authorized personnel or processes.
- D. It ensures that modifications are not made to data by unauthorized personnel or processes.

Answer: B

NEW QUESTION 100

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 104

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 106

You are an Incident manager in Orangesect.Inc. You have been tasked to set up a new extension of your enterprise. The networking, to be done in the new extension, requires different types of cables and an appropriate policy that will be decided by you. Which of the following stages in the Incident handling process involves your decision making?

- A. Preparation
- B. Eradication
- C. Identification
- D. Containment

Answer: A

NEW QUESTION 108

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 110

Fill in the blank with the appropriate phrase. is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time.

- A. Configuration status accounting

Answer: A

NEW QUESTION 113

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 118

Which of the following are the goals of risk management? Each correct answer represents a complete solution. Choose three.

- A. Assessing the impact of potential threats
- B. Identifying the accused
- C. Finding an economic balance between the impact of the risk and the cost of the countermeasure
- D. Identifying the risk

Answer: ACD

NEW QUESTION 120

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 122

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

- A. Legal representative
- B. Technical representative
- C. Lead investigator
- D. Information security representative

Answer: B

NEW QUESTION 126

You work as a Web Administrator for Perfect World Inc. The company is planning to host an E-commerce Web site. You are required to design a security plan for it. Client computers with different operating systems will access the Web server. How will you configure the Web server so that it is secure and only authenticated users are able to access it? Each correct answer represents a part of the solution. Choose two.

- A. Use encrypted authentication.
- B. Use the SSL protocol.
- C. Use the EAP protocol.
- D. Use Basic authentication

Answer: AB

NEW QUESTION 130

Which of the following BCP teams provides clerical support to the other teams and serves as a message center for the user-recovery site?

- A. Security team
- B. Data preparation and records team
- C. Administrative support team
- D. Emergency operations team

Answer: C

NEW QUESTION 135

You have created a team of HR Managers and Project Managers for Blue Well Inc. The team will concentrate on hiring some new employees for the company and improving the organization's overall security by turning employees among numerous job positions. Which of the following steps will you perform to accomplish the task?

- A. Job rotation
- B. Job responsibility
- C. Screening candidates
- D. Separation of duties

Answer: A

NEW QUESTION 139

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 144

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 145

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 148

Rachael is the project manager for a large project in her organization. A new change request has been proposed that will affect several areas of the project. One area of the project change impact is on work that a vendor has already completed. The vendor is refusing to make the changes as they've already completed the project work they were contracted to do. What can Rachael do in this instance?

- A. Threaten to sue the vendor if they don't complete the work.
- B. Fire the vendor for failing to complete the contractual obligation.
- C. Withhold the vendor's payments for the work they've completed.
- D. Refer to the contract agreement for directio

Answer: D

NEW QUESTION 153

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 and training
- B. Evaluation and acceptance
- C. Initiation
- D. Design

Answer: A

NEW QUESTION 155

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 160

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 165

How can you calculate the Annualized Loss Expectancy (ALE) that may occur due to a threat?

- A. Single Loss Expectancy (SLE)/ Exposure Factor (EF)
- B. Asset Value X Exposure Factor (EF)
- C. Exposure Factor (EF)/Single Loss Expectancy (SLE)
- D. Single Loss Expectancy (SLE) X Annualized Rate of Occurrence (ARO)

Answer: D

NEW QUESTION 168

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 173

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 177

You work as a Product manager for Marioiss Inc. You have been tasked to start a project for securing the network of your company. You want to employ configuration management to efficiently manage the procedures of the project. What will be the benefits of employing configuration management for completing this project? Each correct answer represents a complete solution. Choose all that apply.

- A. It provides object, orient, decide and act strategy.
- B. It provides a live documentation of the project.
- C. It provides the risk analysis of project configurations.
- D. It provides the versions for network device

Answer: BD

NEW QUESTION 180

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 183

John works as a security manager for Soft Tech Inc. He is working with his team on the disaster recovery management plan. One of his team members has a doubt related to the most cost effective DRP testing plan. According to you, which of the following disaster recovery testing plans is the most cost-effective and efficient way to identify areas of overlap in the plan before conducting more demanding training exercises?

- A. Full-scale exercise
- B. Walk-through drill
- C. Evacuation drill
- D. Structured walk-through test

Answer: D

NEW QUESTION 184

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 185

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 186

Which of the following is a variant with regard to Configuration Management?

- A. A CI that has the same name as another CI but shares no relationship.
- B. A CI that particularly refers to a hardware specification.

- C. A CI that has the same essential functionality as another CI but a bit different in some small manner.
- D. A CI that particularly refers to a software versio

Answer: C

NEW QUESTION 191

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 Locator (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 194

John is a black hat hacker. FBI arrested him while performing some email scams. Under which of the following US laws will john be charged?

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

Answer: B

NEW QUESTION 198

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 200

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 203

Which of the following types of cyber stalking damage the reputation of their victim and turn other people against them by setting up their own Websites, blogs or user pages for this purpose?

- A. Encouraging others to harass the victim
- B. False accusations
- C. Attempts to gather information about the victim
- D. False victimization

Answer: B

NEW QUESTION 208

Which of the following is used to back up forensic evidences or data folders from the network or locally attached hard disk drives?

- A. WinHex
- B. Vedit
- C. Device Seizure
- D. FAR system

Answer: D

NEW QUESTION 213

You work as a security manager for SoftTech Inc. You along with your team are doing the disaster recovery for your project. Which of the following steps are performed by you for secure recovery based on the extent of the disaster and the organization's recovery ability? Each correct answer represents a part of the solution. Choose three.

- A. Recover to an alternate site for critical functions
- B. Restore full system at an alternate operating site
- C. Restore full system after a catastrophic loss
- D. Recover at the primary operating site

Answer: ACD

NEW QUESTION 214

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 215

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 217

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 customized messages for different groups.
- D. Target senior managers and business process owner

Answer: C

NEW QUESTION 221

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 224

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 management

Answer: B

NEW QUESTION 225

Which of the following governance bodies provides management, operational and technical controls to satisfy security requirements?

- A. Senior Management
- B. Business Unit Manager
- C. Information Security Steering Committee
- D. Chief Information Security Officer

Answer: A

NEW QUESTION 230

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 231

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 232

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 233

Which of the following anti-child pornography organizations helps local communities to create programs and develop strategies to investigate child exploitation?

- A. Internet Crimes Against Children (ICAC)
- B. Project Safe Childhood (PSC)
- C. Anti-Child Porn.org
- D. Innocent Images National Initiative (IINI)

Answer: B

NEW QUESTION 237

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

- A. If you 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 know about your security resources you cannot protect your network

Answer: ABC

NEW QUESTION 239

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 240

An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

- A. Network security policy
- B. Backup policy
- C. Privacy policy
- D. User password policy

Answer: C

NEW QUESTION 244

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 247

Which of the following models uses a directed graph to specify the rights that a subject can transfer to an object or that a subject can take from another subject?

- A. Take-Grant Protection Model
- B. Bell-LaPadula Model
- C. Biba Integrity Model
- D. Access Matrix

Answer: A

NEW QUESTION 249

Which of the following can be done over telephone lines, e-mail, instant messaging, and any other method of communication considered private.

- A. Shielding
- B. Spoofing
- C. Eavesdropping
- D. Packaging

Answer: C

NEW QUESTION 253

In which of the following mechanisms does an authority, within limitations, specify what objects can be accessed by a subject?

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

Answer: B

NEW QUESTION 258

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 259

.....

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

ISSMP Practice Exam Features:

- * ISSMP Questions and Answers Updated Frequently
- * ISSMP Practice Questions Verified by Expert Senior Certified Staff
- * ISSMP Most Realistic Questions that Guarantee you a Pass on Your First Try
- * ISSMP Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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