

ISC2

Exam Questions ISSMP

Information Systems Security Management Professional



NEW QUESTION 1

You work as a Senior Marketing Manger for Umbrella Inc. You find out that some of the software applications on the systems were malfunctioning and also you were not able to access your remote desktop session. You suspected that some malicious attack was performed on the network of the company. You immediately called the incident response team to handle the situation who enquired the Network Administrator to acquire all relevant information regarding the malfunctioning. The Network Administrator informed the incident response team that he was reviewing the security of the network which caused all these problems. Incident response team announced that this was a controlled event not an incident. Which of the following steps of an incident handling process was performed by the incident response team?

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

Answer: D

NEW QUESTION 2

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 3

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 4

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 5

Which of the following terms refers to a mechanism which proves that the sender really sent a particular message?

- A. Non-repudiation
- B. Confidentiality
- C. Authentication
- D. Integrity

Answer: A

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 types of activities can be audited for security? Each correct answer represents a complete solution. Choose three.

- A. Data downloading from the Internet
- B. File and object access
- C. Network logons and logoffs
- D. Printer access

Answer:

BCD

NEW QUESTION 8

Fill in the blank with an appropriate phrase. models address specifications, requirements, and design, verification and validation, and maintenance activities.

A. Life cycle

Answer: A

NEW QUESTION 9

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 10

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 10

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 11

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 12

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 16

Peter works as a Computer Hacking Forensic Investigator. He has been called by an organization to conduct a seminar to give necessary information related to sexual harassment within the work place. Peter started with the definition and types of sexual harassment. He then wants to convey that it is important that records of the sexual harassment incidents should be maintained, which helps in further legal prosecution. Which of the following data should be recorded in this

documentation? Each correct answer represents a complete solution. Choose all that apply.

- A. Names of the victims
- B. Location of each incident
- C. Nature of harassment
- D. Date and time of incident

Answer: ABD

NEW QUESTION 18

Which of the following types of evidence is considered as the best evidence?

- A. A copy of the original document
- B. Information gathered through the witness's senses
- C. The original document
- D. A computer-generated record

Answer: C

NEW QUESTION 21

What are the purposes of audit records on an information system? Each correct answer represents a complete solution. Choose two.

- A. Troubleshooting
- B. Investigation
- C. Upgradation
- D. Backup

Answer: AB

NEW QUESTION 22

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 24

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 29

You work as a security manager for SoftTech Inc. You are conducting a security awareness campaign for your employees. One of the employees of your organization asks you the purpose of the security awareness, training and education program. What will be your answer?

- A. It improves the possibility for career advancement of the IT staff.
- B. It improves the security of vendor relations.
- C. It improves the performance of a company's intranet.
- D. It improves awareness of the need to protect system resource

Answer: D

NEW QUESTION 31

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 33

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 36

Which of the following steps is the initial step in developing an information security strategy?

- A. Perform a technical vulnerabilities assessment.
- B. Assess the current levels of security awareness.
- C. Perform a business impact analysis.
- D. Analyze the current business strateg

Answer: D

NEW QUESTION 40

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 44

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 45

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 47

Which of the following strategies is used to minimize the effects of a disruptive event on a company, and is created to prevent interruptions to normal business activity?

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

Answer: D

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 50

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 51

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 56

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 61

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 65

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 70

Which of the following is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention?

- A. Patent
- B. Utility model
- C. Snooping
- D. Copyright

Answer: A

NEW QUESTION 72

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 75

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 76

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 79

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 83

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 84

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 perfect

Answer: A

NEW QUESTION 86

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

- A. Provide diligent and competent service to principals.
- B. Protect society, the commonwealth, and the infrastructure.
- C. Give guidance for resolving good versus good and bad versus bad dilemmas.
- D. Act honorably, honestly, justly, responsibly, and legally

Answer: ABD

NEW QUESTION 91

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 95

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 99

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 102

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 107

Which of the following administrative policy controls is usually associated with government classifications of materials and the clearances of individuals to access those materials?

- A. Separation of Duties
- B. Due Care
- C. Acceptable Use
- D. Need to Know

Answer: D

NEW QUESTION 108

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 password before 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 Internet.

Answer: A

NEW QUESTION 111

Which of the following security models deal only with integrity? Each correct answer represents a complete solution. Choose two.

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

Answer: BD

NEW QUESTION 116

Rick is the project manager for TTM project. He is in the process of procuring services from vendors. He makes a contract with a vendor in which he precisely specifies the services to be procured, and any changes to the procurement specification will increase the costs to the buyer. Which type of contract is this?

- A. Firm Fixed Price
- B. Fixed Price Incentive Fee
- C. Cost Plus Fixed Fee Contract
- D. Fixed Price with Economic Price Adjustment

Answer: A

NEW QUESTION 118

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 122

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 125

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 130

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 135

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 depends on what the termination clause of the contract stipulates.
- D. No, the ZAS Corporation did not complete all of the work.

Answer: C

NEW QUESTION 136

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 141

Fill in the blank with an appropriate phrase. is used to provide security mechanisms for the storage, processing, and transfer of data.

A. Data classification

Answer: A

NEW QUESTION 145

Which of the following are examples of physical controls used to prevent unauthorized access to sensitive materials?

- A. Thermal alarm systems
- B. Closed circuit cameras
- C. Encryption
- D. Security Guards

Answer: ABD

NEW QUESTION 150

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 151

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 152

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 153

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 157

Which of the following methods for identifying appropriate BIA interviewees' includes examining the organizational chart of the enterprise to understand the functional positions?

- A. Organizational chart reviews
- B. Executive management interviews
- C. Overlaying system technology
- D. Organizational process models

Answer: A

NEW QUESTION 160

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 163

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 167

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 170

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 171

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 172

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 data

Answer: ABC

NEW QUESTION 174

Which of the following statements is true about auditing?

- A. It is used to protect the network against virus attacks.
- B. It is used to track user accounts for file and object access, logon attempts, etc.
- C. It is used to secure the network or the computers on the network.
- D. It is used to prevent unauthorized access to network resource

Answer: B

NEW QUESTION 179

Your project team has identified a project risk that must be responded to. The risk has been recorded in the risk register and the project team has been discussing potential risk responses for the risk event. The event is not likely to happen for several months but the probability of the event is high. Which one of the following is a valid response to the identified risk event?

- A. Earned value management
- B. Risk audit
- C. Technical performance measurement
- D. Corrective action

Answer: D

NEW QUESTION 181

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 182

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 direction

Answer: D

NEW QUESTION 187

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 188

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 192

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 196

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 201

Which of the following elements of BCP process includes the areas of plan implementation, plan testing, and ongoing plan maintenance, and also involves defining and documenting the continuity strategy?

- A. Business continuity plan development
- B. Business impact assessment
- C. Scope and plan initiation
- D. Plan approval and implementation

Answer: A

NEW QUESTION 202

Which of the following Acts enacted in United States allows the FBI to issue National Security Letters (NSLs) to Internet service providers (ISPs) ordering them to disclose records about their customers?

- A. Electronic Communications Privacy Act of 1986
- B. Wiretap Act
- C. Computer Fraud and Abuse Act
- D. Economic Espionage Act of 1996

Answer: A

NEW QUESTION 205

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

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 210

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 213

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 218

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 221

Which of the following are the responsibilities of a custodian 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. Running regular backups and routinely testing the validity of the backup data
- C. Controlling access, adding and removing privileges for individual users
- D. Performing data restoration from the backups when necessary

Answer: BCD

NEW QUESTION 225

Which of the following statements are true about a hot site? Each correct answer represents a complete solution. Choose all that apply.

- A. It can be used within an hour for data recovery.
- B. It is cheaper than a cold site but more expensive than a warm site.
- C. It is the most inexpensive backup site.
- D. It is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data.

Answer: AD

NEW QUESTION 228

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 233

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 236

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 240

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 242

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 247

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 249

Which of the following methods can be helpful to eliminate social engineering threat? Each correct answer represents a complete solution. Choose three.

- A. Password policies
- B. Vulnerability assessments
- C. Data encryption
- D. Data classification

Answer: ABD

NEW QUESTION 253

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 257

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 259

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 260

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 262

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 266

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 269

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 273

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 276

Which of the following refers to the ability to ensure that the data is not modified or tampered with?

- A. Availability
- B. Non-repudiation
- C. Integrity
- D. Confidentiality

Answer: C

NEW QUESTION 278

You work as the project manager for Bluewell Inc. You are working on NGQQ Project for your company. You have completed the risk analysis processes for the risk events. You and the project team have created risk responses for most of the identified project risks. Which of the following risk response planning techniques will you use to shift the impact of a threat to a third party, together with the responses?

- A. Risk mitigation
- B. Risk acceptance
- C. Risk avoidance
- D. Risk transference

Answer: D

NEW QUESTION 280

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

- A. Model

Answer: A

NEW QUESTION 282

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 284

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 289

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 294

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 295

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 297

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 298

.....

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](#)