

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

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 6

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

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

Answer: D

NEW QUESTION 7

Which of the following subphases are defined in the maintenance phase of the life cycle models?

- A. Change control
- B. Configuration control
- C. Request control
- D. Release control

Answer: ACD

NEW QUESTION 8

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 9

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 10

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 10

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 11

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 14

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 19

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 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 25

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 28

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 29

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 33

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 38

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

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

Answer: AC

NEW QUESTION 42

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 45

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

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 54

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 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

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 63

James works as a security manager for SoftTech Inc. He has been working on the continuous process improvement and on the ordinal scale for measuring the maturity of the organization involved in the software processes. According to James, which of the following maturity levels of software CMM focuses on the continuous process improvement?

- A. Repeatable level
- B. Defined level
- C. Initiating level
- D. Optimizing level

Answer: D

NEW QUESTION 67

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 70

Which of the following enables an inventor to legally enforce his right to exclude others from using his invention?

- A. Spam
- B. Patent
- C. Artistic license
- D. Phishing

Answer: B

NEW QUESTION 71

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 74

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 79

Which of the following ports is the default port for Layer 2 Tunneling Protocol (L2TP) ?

- A. UDP port 161
- B. TCP port 443
- C. TCP port 110
- D. UDP port 1701

Answer: D

NEW QUESTION 84

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 87

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 90

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 94

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 96

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 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 102

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 105

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 106

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 111

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 specify 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 113

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 117

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 122

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 123

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 125

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 130

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 132

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

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

Answer: ABC

NEW QUESTION 134

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 138

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 142

Which of the following security issues does the Bell-La Padula model focus on?

- A. Authentication
- B. Confidentiality
- C. Integrity
- D. Authorization

Answer: B

NEW QUESTION 143

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 145

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 147

Fill in the blank with an appropriate phrase. _____ is a branch of forensic science pertaining to legal evidence found in computers and digital storage media.

- A. Computer forensics

Answer: A

NEW QUESTION 152

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. Correctiveaction

Answer: D

NEW QUESTION 153

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 157

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 162

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

Which of the following protocols are used to provide secure communication between a client and a server over the Internet? Each correct answer represents a part of the solution. Choose two.

- A. TLS
- B. HTTP
- C. SNMP
- D. SSL

Answer: AD

NEW QUESTION 167

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

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 171

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 175

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 176

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 178

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 182

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

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

Answer: C

NEW QUESTION 187

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 189

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 192

Your 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 194

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 196

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 199

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 200

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 201

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 205

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

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

Answer: C

NEW QUESTION 209

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 212

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

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

Answer: B

NEW QUESTION 217

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 218

Which of the following is the default port for Secure Shell (SSH)?

- A. UDP port 161
- B. TCP port 22
- C. UDP port 138
- D. TCP port 443

Answer: B

NEW QUESTION 223

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 228

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

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

Answer: B

NEW QUESTION 230

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 234

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 236

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 240

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 242

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 243

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 244

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 246

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 248

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 253

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

- A. Model

Answer: A

NEW QUESTION 256

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 257

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 258

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 260

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 263

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

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

Answer: ABC

NEW QUESTION 266

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 267

.....

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](#)