

Exam Questions ISSMP

Information Systems Security Management Professional

<https://www.2passeasy.com/dumps/ISSMP/>



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 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 4

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 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 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 7

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 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

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

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

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

Answer: BCDE

NEW QUESTION 10

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 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 14

Which of the following refers to an information security document that is used in the United States Department of Defense (DoD) to describe and accredit networks and systems?

- A. SSAA
- B. FITSAF
- C. FIPS
- D. TCSEC

Answer: A

NEW QUESTION 19

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 21

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 24

You are responsible for network and information security at a metropolitan police station. The most important concern is that unauthorized parties are not able to access data. What is this called?

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

Answer: D

NEW QUESTION 25

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 29

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 31

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

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

Answer: B

NEW QUESTION 33

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 37

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 39

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 43

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 47

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 48

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 49

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 51

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

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

Answer: C

NEW QUESTION 56

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 61

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 63

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 64

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 65

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 66

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 67

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 69

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 72

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 77

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 81

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 82

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

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

Answer: ABCDE

NEW QUESTION 84

Which of the following tools works by using standard set of MS-DOS commands and can create an MD5 hash of an entire drive, partition, or selected files?

- A. Device Seizure
- B. Ontrack
- C. DriveSpy
- D. Forensic Sorter

Answer: C

NEW QUESTION 86

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 87

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 89

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 94

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 98

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 103

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 104

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 107

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 112

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 115

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

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

Answer: B

NEW QUESTION 116

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

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

Answer: D

NEW QUESTION 119

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 124

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

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

Answer: D

NEW QUESTION 129

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 132

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 134

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

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

Answer: A

NEW QUESTION 136

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 137

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 139

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 142

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 145

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 147

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 150

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 154

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 155

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 157

Which of the following authentication protocols provides support for a wide range of authentication methods, such as smart cards and certificates?

- A. PAP
- B. EAP
- C. MS-CHAP v2
- D. CHAP

Answer: B

NEW QUESTION 158

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 161

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

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

Answer: C

NEW QUESTION 164

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 167

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

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

Answer: C

NEW QUESTION 172

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

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

Answer: B

NEW QUESTION 174

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 178

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

- A. OPSEC assessment

Answer: A

NEW QUESTION 183

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 184

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 189

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 193

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 195

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 198

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 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 network.

Answer: BC

NEW QUESTION 203

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 206

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

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 211

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 214

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

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

Answer: C

NEW QUESTION 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 222

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 223

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 224

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 227

Which of the following rated systems of the Orange book has mandatory protection of the TCB?

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

Answer: A

NEW QUESTION 228

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

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

Answer: C

NEW QUESTION 232

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 235

Which of the following processes provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and the security posture of a system or site?

- A. NSA-IAM
- B. DITSCAP
- C. ASSET
- D. NIACAP

Answer: D

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 243

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

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

Answer: C

NEW QUESTION 244

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 246

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 248

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 251

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 256

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

A. Model

Answer: A

NEW QUESTION 258

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 259

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 263

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 268

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 273

Which of the following plans is designed to protect critical business processes from natural or man-made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes?

- A. Business continuity plan
- B. Crisis communication plan
- C. Contingency plan
- D. Disaster recovery plan

Answer: A

NEW QUESTION 278

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

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

Answer: B

NEW QUESTION 280

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 285

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual ISSMP Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the ISSMP Product From:

<https://www.2passeasy.com/dumps/ISSMP/>

Money Back Guarantee

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