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 penetration testing phases involves reconnaissance or data gathering?

A. Attack phase
B. Pre-attack phase
C. Post-attack phase
D. Out-attack phase

Answer: B

NEW QUESTION 4
Which of the following protocols is used with a tunneling protocol to provide security?

A. FTP
B. IPX/SPX
C. IPSec
D. EAP

Answer: C

NEW QUESTION 5
Which of the following BCP teams is the first responder and deals with the immediate effects of the disaster?

A. Emergency-management team
B. Damage-assessment team
C. Off-site storage team
D. Emergency action team

Answer: D

NEW QUESTION 6
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 7
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 8
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. Requirementanalysis

Answer: C

NEW QUESTION 9
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 10
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 10
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 15
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 19
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 22
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 27
Change Management is used to ensure that standardized methods and procedures are used for efficient handling of all changes. Who decides the category of a change?

A. The Problem Manager
B. The Process Manager
C. The Change Manager
D. The Service Desk
E. The Change Advisory Board

Answer: C

NEW QUESTION 31
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 34
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 37
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 41
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 46
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 47
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 52
Which of the following statements about Due Care policy is true?

A. It is a method used to authenticate users on a network.
B. It is a method for securing database servers.
C. It identifies the level of confidentiality of information.
D. It provides information about new viruse

Answer: C

NEW QUESTION 55
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 57
Which of the following deals is a binding agreement between two or more persons that is enforceable by law?

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

Answer: C

NEW QUESTION 60
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 65
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 69
Which of the following processes will you involve to perform the active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known
and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures?

A. Penetration testing
B. Risk analysis
C. Baselining
D. Compliance checking

Answer: A

NEW QUESTION 73
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 77
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 81
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 86
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 90
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 92
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 93
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 97
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 100
Which of the following are the responsibilities of the owner with regard to data in an information classification program? Each correct answer represents a complete

solution. Choose three.

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

Answer: ABC

NEW QUESTION 103
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 106
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 107
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 111
Which of the following statements reflect the 'Code of Ethics Preamble' in the '(ISC)2 Code of Ethics'? Each correct answer represents a complete solution. Choose all that apply.

A. Strict adherence to this Code is a condition of certification.
B. Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
C. Advance and protect the profession.
D. Provide diligent and competent service to principal

Answer: AB

NEW QUESTION 113
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 115
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 118
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 123
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 124
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 129
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 130
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 131
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 133
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 138
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 140
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 142
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 145
You are the Network Administrator for a software company. Due to the nature of your company's business, you have a significant number of highly computer savvy users. However, you have still decided to limit each user access to only those resources required for their job, rather than give wider access to the technical users (such as tech support and software engineering personnel).
What is this an example of?

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

Answer: B

NEW QUESTION 149
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 152
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 154
Which of the following are known as the three laws of OPSEC? Each correct answer represents a part of the solution. Choose three.

A. Ifyou 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 knowabout your security resources you cannot protect your networ

Answer: ABC

NEW QUESTION 155
Which of the following processes is used by remote users to make a secure connection to internal resources after establishing an Internet connection?

A. Packet filtering
B. Tunneling
C. Packet sniffing
D. Spoofing

Answer: B

NEW QUESTION 160
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 162
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 167
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 169
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 171
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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 FirstTry

* ISSMP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The ISSMP Practice Test Here