CISSP-ISSMP.exam.130q

Number: CISSP-ISSMP
Passing Score: 800
Time Limit: 120 min
File Version: 1

ISC ISSMP

https://www.gratisexam.com/

ISSMP®: Information Systems Security Management Professional

Exam A

QUESTION 1
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following analysis provides a foundation for measuring investment of time, money and human resources required to achieve a particular outcome?

A. Vulnerability analysis
B. Cost-benefit analysis
C. Gap analysis
D. Requirement analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
A contract cannot have provisions for which one of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
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 resources.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Electronic communication technology refers to technology devices, such as computers and cell phones, used to facilitate communication. Which of the following is/ are a type of electronic communication? Each correct answer represents a complete solution. Choose all that apply.

A. Internet telephony
B. Instant messaging
C. Electronic mail
D. Post-it note
E. Blogs
F. Internet teleconferencing

Correct Answer: ABCEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
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 strategy.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following statements about the integrity concept of information security management are true? Each correct answer represents a complete solution. Choose three.

A. It ensures that unauthorized modifications are not made to data by authorized personnel or processes.
B. It determines the actions and behaviors of a single individual within a system
C. It ensures that modifications are not made to data by unauthorized personnel or processes.
D. It ensures that internal information is consistent among all subentities and also consistent with the real-world, external situation.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
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 whom.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following roles is responsible for review and risk analysis of all contracts on a regular basis?

A. The Configuration Manager
B. The Supplier Manager
C. The Service Catalogue Manager
D. The IT Service Continuity Manager

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which of the following statements is related with the first law of OPSEC?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which of the following policies helps reduce the potential damage from the actions of one person?

A. CSA
B. Risk assessment
C. Separation of duties
D. Internal audit

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
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

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which of the following is a process of monitoring data packets that travel across a network?

A. Password guessing
B. Packet sniffing
C. Shielding
D. Packet filtering

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
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 change control system

D. Project integration management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following statements reflect the 'Code of Ethics Canons' in the '(ISC)2 Code of Ethics'? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
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

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Which of the following statements about Due Care policy is true?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
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

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
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)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Which of the following sections come under the ISO/IEC 27002 standard?

A. Financial assessment
B. Asset management
C. Security policy
D. Risk assessment

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Which of the following U.S. Federal laws addresses computer crime activities in communication lines, stations, or systems?

A. 18 U.S.C. 1362
B. 18 U.S.C. 1030

C. 18 U.S.C. 1029
D. 18 U.S.C. 2701
E. 18 U.S.C. 2510

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
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

Correct Answer: ABCDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
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. Minimize the 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 disaster.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
SIMULATION
Fill in the blank with an appropriate phrase._____ is used to provide security mechanisms for the storage, processing, and transfer of data.

Correct Answer: Data classification
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
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

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which of the following security issues does the Bell-La Padula model focus on?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which of the following are the types of access controls? Each correct answer represents a complete solution. Choose three.

A. Administrative
B. Automatic
C. Physical
D. Technical

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 69
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
A Web-based credit card company had collected financial and personal details of Mark before issuing him a credit card. The company has now provided Mark's financial and personal details to another company. Which of the following Internet laws has the credit card issuing company violated?

A. Copyright law
B. Trademark law
C. Privacy law
D. Security law

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
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.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
Which of the following statements are true about security risks? Each correct answer represents a complete solution. Choose three.

A. They can be analyzed and measured by the risk analysis process.
B. They can be removed completely by taking proper actions.
C. They can be mitigated by reviewing and taking responsible actions based on possible risks.
D. They are considered an indicator of threats coupled with vulnerability.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which of the following BCP teams provides clerical support to the other teams and serves as a message center for the user-recovery site?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
You have created a team of HR Managers and Project Managers for Blue Well Inc. The team will concentrate on hiring some new employees for the company and improving the organization's overall security by turning employees among numerous job positions. Which of the following steps will you perform to accomplish the task?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Your project has several risks that may cause serious financial impact should they happen. You have studied the risk events and made some potential risk responses for the risk events but management wants you to do more. They'd like for you to create some type of a chart that identified the risk probability and impact with a financial amount for each risk event. What is the likely outcome of creating this type of chart?

A. Quantitative analysis
B. Contingency reserve
C. Risk response
D. Risk response plan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
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

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
Which of the following are the responsibilities of the owner with regard to data in an information classification program? Each correct answer represents a complete solution. Choose three.

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

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
You work as the Network Administrator for a defense contractor. Your company works with sensitive materials and all IT personnel have at least a secret level clearance. You are still concerned that one individual could perhaps compromise the network (intentionally or unintentionally) by setting up improper or unauthorized remote access. What is the best way to avoid this problem?

A. Implement separation of duties.
B. Implement RBAC.
C. Implement three way authentication.
D. Implement least privileges.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Which of the following statements is true about auditing?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
SIMULATION
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.

Correct Answer: Computer forensics
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Your project team has identified a project risk that must be responded to. The risk has been recorded in the risk register and the project team has been discussing potential risk responses for the risk event. The event is not likely to happen for several months but the probability of the event is high. Which one of the following is a valid response to the identified risk event?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Rachael is the project manager for a large project in her organization. A new change request has been proposed that will affect several areas of the project. One area of the project change impact is on work that a vendor has already completed. The vendor is refusing to make the changes as they've already completed the project work they were contracted to do. What can Rachael do in this instance?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88

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?

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
SIMULATION
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.

Correct Answer: OPSEC assessment
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Which of the following Acts enacted in United States allows the FBI to issue National Security Letters (NSLs) to Internet service providers (ISPs) ordering them to disclose records about their customers?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
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 devices.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
You company suspects an employee of sending unauthorized emails to competitors. These emails are alleged to contain confidential company dat a. 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
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

Correct Answer: BDEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which of the following backup sites takes the longest recovery time?

A. Cold site
B. Hot site
C. Warm site
D. Mobile backup site

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
The incident response team has turned the evidence over to the forensic team. Now, it is the time to begin looking for the ways to improve the incident response process for next time. What are the typical areas for improvement? Each correct answer represents a complete solution. Choose all that apply.

A. Information dissemination policy
B. Electronic monitoring statement
C. Additional personnel security controls
D. Incident response plan

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Which of the following is a variant with regard to Configuration Management?

A. A CI that has the same name as another CI but shares no relationship.
B. A CI that particularly refers to a hardware specification.
C. A CI that has the same essential functionality as another CI but a bit different in some small manner.
D. A CI that particularly refers to a software version.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
You work as a Forensic Investigator. Which of the following rules will you follow while working on a case? Each correct answer represents a part of the solution. Choose all that apply.

A. Prepare a chain of custody and handle the evidence carefully.

B. Examine original evidence and never rely on the duplicate evidence.
C. Never exceed the knowledge base of the forensic investigation.
D. Follow the rules of evidence and never temper with the evidence.

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
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

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
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 Locater (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.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
John is a black hat hacker. FBI arrested him while performing some email scams. Under which of the following US laws will john be charged?

A. 18 U.S.C. 1362
B. 18 U.S.C. 1030
C. 18 U.S.C. 2701
D. 18 U.S.C. 2510

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
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 worm 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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
NIST Special Publication 800-50 is a security awareness program. It is designed for those people who are currently working in the information technology field and want information on security policies. Which of the following are some of its critical steps? Each correct answer represents a complete solution. Choose two.

A. Awareness and Training Material Effectiveness
B. Awareness and Training Material Development

C. Awareness and Training Material Implementation
D. Awareness and Training Program Design

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
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. Video surveillance on all areas with computers.
B. Use laptop locks.
C. Appoint a security guard.
D. Smart card access to all areas with computers.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
Shoulder surfing is a type of in-person attack in which the attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard of an employee's computer while he is typing in his password at any access point such as a terminal/Web site. Which of the following is violated in a shoulder surfing attack?

A. Availability
B. Confidentiality
C. Integrity
D. Authenticity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
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

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 115
Mark is the project manager of the NHQ project in Spartech Inc. The project has an asset valued at $195,000 and is subjected to an exposure factor of 35 percent. What will be the Single Loss Expectancy of the project?

https://www.gratisexam.com/

A. $92,600
B. $67,250
C. $68,250
D. $72,650

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
You work as a security manager for SoftTech Inc. You along with your team are doing the disaster recovery for your project. Which of the following steps are performed by you for secure recovery based on the extent of the disaster and the organization's recovery ability? Each correct answer represents a part of the solution. Choose three.

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

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
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

Correct Answer: ACDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
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

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
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

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
You work as a security manager for SoftTech Inc. You are conducting a security awareness campaign for your employees. Which of the following ideas will you consider the best when conducting a security awareness campaign?

A. Target system administrators and the help desk.
B. Provide technical details on exploits.
C. Provide customized messages for different groups.
D. Target senior managers and business process owners.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
Which of the following SDLC phases consists of the given security controls. Misuse Case Modeling Security Design and Architecture Review Threat and Risk Modeling Security Requirements and Test Cases Generation

A. Design
B. Maintenance
C. Deployment
D. Requirements Gathering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
Which of the following liabilities is a third-party liability in which an individual may be responsible for an action by another party?

A. Relational liability
B. Engaged liability
C. Contributory liability
D. Vicarious liability

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
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

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
Which of the following are examples of administrative controls that involve all levels of employees within an organization and determine which users have access to what resources and information? Each correct answer represents a complete solution. Choose three.

A. Employee registration and accounting
B. Disaster preparedness and recovery plans
C. Network authentication
D. Training and awareness
E. Encryption

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference: