ISC.CISSP-ISSMP.by.Dany.154q

Number: CISSP-ISSMP
Passing Score: 800
Time Limit: 120
File Version: 21.0

Exam Code: CISSP-ISSMP
Exam Name: Information Systems Security Management Professional

Exam A

QUESTION 1
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:

QUESTION 2
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:

QUESTION 3
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:

QUESTION 4
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:

QUESTION 5
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:

QUESTION 6
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:

QUESTION 7
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:

QUESTION 8
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:

QUESTION 9
Mark is the project manager of the NHQ project in Spartech Inc. The project has an asset valued at $195,000 and is subjected to an exposure factor of 35 percent. What will be the Single Loss Expectancy of the project?

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

Correct Answer: C
Section:

QUESTION 10
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:

QUESTION 11
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:

QUESTION 12
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:

QUESTION 13
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:

QUESTION 14
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: C, D
Section:

QUESTION 15
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:

QUESTION 16
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:

QUESTION 17
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: A, B, D
Section:

QUESTION 18
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

Correct Answer: D
Section:

QUESTION 19
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

Correct Answer: D
Section:

QUESTION 20
Which of the following involves changing data prior to or during input to a computer in an effort to commit fraud?

A. Data diddling
B. Wiretapping
C. Eavesdropping
D. Spoofing

Correct Answer: A
Section:

QUESTION 21
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

Correct Answer: B
Section:

QUESTION 22
Mark works as a security manager for SoftTech Inc. He is involved in the BIA phase to create a document to be used to help understand what impact a disruptive event would have on the business. The impact might be financial or operational. Which of the following are the objectives related to the above phase in which
Mark is involved? Each correct answer represents a part of the solution. Choose three.

A. Resource requirements identification
B. Criticality prioritization
C. Down-time estimation
D. Performing vulnerability assessment

Correct Answer: A, B, C
Section:

QUESTION 23
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

Correct Answer: D
Section:

QUESTION 24
Which of the following protocols is used with a tunneling protocol to provide security?

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

Correct Answer: C
Section:

QUESTION 25
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

Correct Answer: A, C, D
Section:

QUESTION 26
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

Correct Answer: A
Section:

QUESTION 27
Which of the following characteristics are described by the DIAP Information Readiness Assessment function? Each correct answer represents a complete solution. Choose all that apply.

A. It performs vulnerability/threat analysis assessment.
B. It identifies and generates IA requirements.
C. It provides data needed to accurately assess IA readiness.
D. It provides for entry and storage of individual system data.

Correct Answer: A, B, C
Section:

QUESTION 28
Joseph works as a Software Developer for Web Tech Inc. He wants to protect the algorithms and the techniques of programming that he uses in developing an application. Which of the following laws are used to protect a part of software?

A. Code Security law
B. Trademark laws
C. Copyright laws
D. Patent laws

Correct Answer: D
Section:

QUESTION 29
Which of the following is the best method to stop vulnerability attacks on a Web server?

A. Using strong passwords
B. Configuring a firewall

C. Implementing the latest virus scanner
D. Installing service packs and updates

Correct Answer: D
Section:

QUESTION 30
Which of the following is NOT a valid maturity level of the Software Capability Maturity Model (CMM)?

A. Managed level
B. Defined level
C. Fundamental level
D. Repeatable level

Correct Answer: C
Section:

QUESTION 31
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

Correct Answer: D
Section:

QUESTION 32
Which of the following security models dictates that subjects can only access objects through applications?

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

Correct Answer: C
Section:

QUESTION 33
Which of the following relies on a physical characteristic of the user to verify his identity?

A. Social Engineering
B. Kerberos v5
C. Biometrics
D. CHAP

Correct Answer: C
Section:

QUESTION 34
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

Correct Answer: B, C, D
Section:

QUESTION 35
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

Correct Answer: D
Section:

QUESTION 36
Which of the following laws is the first to implement penalties for the creator of viruses, worms, and other types of malicious code that causes harm to the computer systems?

A. Gramm-Leach-Bliley Act
B. Computer Fraud and Abuse Act
C. Computer Security Act
D. Digital Millennium Copyright Act

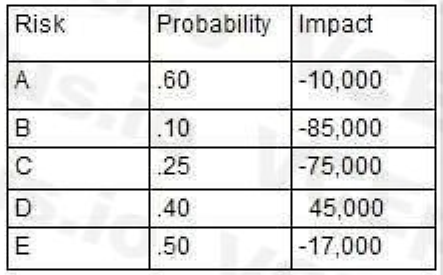
Correct Answer: B
Section:

QUESTION 37
SIMULATION Fill in the blank with an appropriate phrase.________ models address specifications, requirements, and design, verification and validation, and maintenance activities.

A. Life cycle

Correct Answer: A
Section:

QUESTION 38
You are the project manager of the GHE Project. You have identified the following risks with the characteristics as shown in the following figure:



Risk	Probability	Impact
A	.60	-10,000
B	.10	-85,000
C	.25	-75,000
D	.40	45,000
E	.50	-17,000

How much capital should the project set aside for the risk contingency reserve?

A. $142,000
B. $232,000
C. $41,750
D. $23,750

Correct Answer: D
Section:

QUESTION 39
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.

Correct Answer: A, D
Section:

QUESTION 40
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

Correct Answer: B, C, D, E
Section:

QUESTION 41
Which of the following processes is described in the statement below? "It is the process of implementing risk response plans, tracking identified risks, monitoring residual risk, identifying new risks, and evaluating risk process effectiveness throughout the project."

A. Monitor and Control Risks

B. Identify Risks
C. Perform Qualitative Risk Analysis
D. Perform Quantitative Risk Analysis

Correct Answer: A
Section:

QUESTION 42
Walter is the project manager of a large construction project. He'll be working with several vendors on the project. Vendors will be providing materials and labor for several parts of the project. Some of the works in the project are very dangerous so Walter has implemented safety requirements for all of the vendors and his own project team. Stakeholders for the project have added new requirements, which have caused new risks in the project. A vendor has identified a new risk that could affect the project if it comes into fruition. Walter agrees with the vendor and has updated the risk register and created potential risk responses to mitigate the risk. What should Walter also update in this scenario considering the risk event?

A. Project contractual relationship with the vendor
B. Project management plan
C. Project communications plan
D. Project scope statement

Correct Answer: B
Section:

QUESTION 43
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

Correct Answer: C
Section:

QUESTION 44
Which of the following security controls will you use for the deployment phase of the SDLC to build secure software? Each correct answer represents a complete solution. Choose all that apply.

A. Vulnerability Assessment and Penetration Testing
B. Security Certification and Accreditation (C&A)
C. Change and Configuration Control
D. Risk Adjustments

Correct Answer: A, B, D
Section:

QUESTION 45
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

Correct Answer: A
Section:

QUESTION 46
Peter works as a Computer Hacking Forensic Investigator. He has been called by an organization to conduct a seminar to give necessary information related to sexual harassment within the work place. Peter started with the definition and types of sexual harassment. He then wants to convey that it is important that records of the sexual harassment incidents should be maintained, which helps in further legal prosecution. Which of the following data should be recorded in this documentation? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: A, B, D
Section:

QUESTION 47
Which of the following types of evidence is considered as the best evidence?

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

Correct Answer: C
Section:

QUESTION 48
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

Correct Answer: A, B
Section:

QUESTION 49
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:

QUESTION 50
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:

QUESTION 51
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:

QUESTION 52
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:

QUESTION 53
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:

QUESTION 54
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:

QUESTION 55
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:

QUESTION 56
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: A, B, C, E, F
Section:

QUESTION 57
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:

QUESTION 58
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:

QUESTION 59
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:

QUESTION 60
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: A, C, D
Section:

QUESTION 61
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:

QUESTION 62
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:

QUESTION 63
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: A, C
Section:

QUESTION 64
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:

QUESTION 65
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:

QUESTION 66
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:

QUESTION 67
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: A, B, C
Section:

QUESTION 68
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:

QUESTION 69
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:

QUESTION 70
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: A, C, D
Section:

QUESTION 71
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:

QUESTION 72
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:

QUESTION 73
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:

QUESTION 74
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:

QUESTION 75
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: B, C, D
Section:

QUESTION 76
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:

QUESTION 77
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:

QUESTION 78
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:

QUESTION 79
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:

QUESTION 80
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:

QUESTION 81
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:

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

Correct Answer: A, B, C, D, E
Section:

QUESTION 83
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:

QUESTION 84
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:

QUESTION 85
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.

Correct Answer: A
Section:

QUESTION 86
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)

Correct Answer: D
Section:

QUESTION 87
Which of the following security models deal only with integrity? Each correct answer represents a complete solution. Choose two.

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

Correct Answer: B, D
Section:

QUESTION 88
Rick is the project manager for TTM project. He is in the process of procuring services from vendors. He makes a contract with a vendor in which he precisely specify the services to be procured, and any changes to the procurement specification will increase the costs to the buyer. Which type of contract is this?

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

Correct Answer: A
Section:

QUESTION 89
You are an Incident manager in Orangesect.Inc. You have been tasked to set up a new extension of your enterprise. The networking, to be done in the new extension, requires different types of cables and an appropriate policy that will be decided by you. Which of the following stages in the Incident handling process involves your decision making?

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

Correct Answer: A
Section:

QUESTION 90
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

Correct Answer: A

Section:

QUESTION 91
SIMULATION
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

Correct Answer: A
Section:

QUESTION 92
SIMULATION
Fill in the blank with an appropriate phrase.____________ is the process of using a strategy and plan of what patches should be applied to which systems at a specified time. Correct

A. Patch management

Correct Answer: A
Section:

QUESTION 93
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. Disaster recovery plan
B. Contingency plan
C. Continuity of Operations Plan
D. Business continuity plan

Correct Answer: B
Section:

QUESTION 94
Which of the following BCP teams handles financial arrangement, public relations, and media inquiries in the time of disaster recovery?

A. Software team
B. Off-site storage team
C. Applications team
D. Emergency-management team

Correct Answer: D
Section:

QUESTION 95
SIMULATION
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

Correct Answer: A
Section:

QUESTION 96
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:

QUESTION 97
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:

QUESTION 98
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: A, B, D
Section:

QUESTION 99
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:

QUESTION 100

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: A, B
Section:

QUESTION 101

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: A, C, D
Section:

QUESTION 102

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:

QUESTION 103

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:

QUESTION 104

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:

QUESTION 105
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: A, B
Section:

QUESTION 106
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: A, C, D
Section:

QUESTION 107
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:

QUESTION 108
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:

QUESTION 109
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:

QUESTION 110
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:

QUESTION 111
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:

QUESTION 112
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:

QUESTION 113
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: A, C, D
Section:

QUESTION 114
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:

QUESTION 115
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: A, B, C
Section:

QUESTION 116
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:

QUESTION 117
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:

QUESTION 118
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: B, C, D
Section:

QUESTION 119
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: B, C
Section:

QUESTION 120
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:

QUESTION 121
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: A, D
Section:

QUESTION 122
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: B, D
Section:

QUESTION 123
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: A, C, D
Section:

QUESTION 124
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: A, C, D, E
Section:

QUESTION 125
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:

QUESTION 126
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: A, B, C
Section:

QUESTION 127
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: A, B, D
Section:

QUESTION 128
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:

QUESTION 129
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:

QUESTION 130
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:

QUESTION 131
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:

QUESTION 132
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:

QUESTION 133
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:

QUESTION 134
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:

QUESTION 135
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: A, B, D
Section:

QUESTION 136
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

Correct Answer: D
Section:

QUESTION 137
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

Correct Answer: A
Section:

QUESTION 138
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

Correct Answer: C
Section:

QUESTION 139
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

Correct Answer: D
Section:

QUESTION 140
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

Correct Answer: B
Section:

QUESTION 141
Tomas is the project manager of the QWS Project and is worried that the project stakeholders will want to change the project scope frequently. His fear is based on the many open issues in the project and how the resolution

of the issues may lead to additional project changes. On what document are Tomas and the stakeholders working in this scenario?

A. Communications management plan
B. Change management plan
C. Issue log
D. Risk management plan

Correct Answer: B
Section:

QUESTION 142
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

Correct Answer: A
Section:

QUESTION 143
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

Correct Answer: C
Section:

QUESTION 144
Which of the following anti-child pornography organizations helps local communities to create programs and develop strategies to investigate child exploitation?

A. Internet Crimes Against Children (ICAC)
B. Project Safe Childhood (PSC)
C. Anti-Child Porn.org
D. Innocent Images National Imitative (IINI)

Correct Answer: B
Section:

QUESTION 145
You work as the project manager for Bluewell Inc. You are working on NGQQ Project for your company. You have completed the risk analysis processes for the risk events. You and the project team have created risk responses for most of the identified project risks. Which of the following risk response planning techniques will you use to shift the impact of a threat to a third party, together with the responses?

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

Correct Answer: D
Section:

QUESTION 146
SIMULATION
Fill in the blank with an appropriate word. _________ are used in information security to formalize security policies.

A. Models

Correct Answer: A
Section:

QUESTION 147
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.

Correct Answer: A, B, C
Section:

QUESTION 148
Eric is the project manager of the NQQ Project and has hired the ZAS Corporation to complete part of the project work for Eric's organization. Due to a change request the ZAS Corporation is no longer needed on the project even though they have completed nearly all of the project work. Is Eric's organization liable to pay the ZAS Corporation for the work they have completed so far on the project?

A. Yes, the ZAS Corporation did not choose to terminate the contract work.
B. It depends on what the outcome of a lawsuit will determine.
C. It depends on what the termination clause of the contract stipulates.
D. No, the ZAS Corporation did not complete all of the work.

Correct Answer: C
Section:

QUESTION 149
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

Correct Answer: A, C, D
Section:

QUESTION 150
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

Correct Answer: C
Section:

QUESTION 151
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: A, B, C
Section:

QUESTION 152
In which of the following alternative processing sites is the backup facility maintained in a constant order, with a full complement of servers, workstations, and communication links ready to assume the primary operations responsibility?

A. Mobile Site
B. Cold Site
C. Warm Site
D. Hot Site

Correct Answer: D
Section:

QUESTION 153
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

Correct Answer: B
Section:

QUESTION 154
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

Correct Answer: B
Section: