CISSP-ISSMP.135q

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

GRATIS EXAM
Free Practice Exams
https://www.gratisexam.com/

ISSMP

ISSMP®: Information Systems Security Management Professional

Exam A

QUESTION 1
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: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following terms refers to a mechanism which proves that the sender really sent a particular message?

GRATIS EXAM
Free Practice Exams
https://www.gratisexam.com/

A. Non-repudiation
B. Confidentiality
C. Authentication
D. Integrity

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
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: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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: (none)
Explanation

Explanation/Reference:

QUESTION 5
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: (none)
Explanation

Explanation/Reference:

QUESTION 6
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: (none)
Explanation

Explanation/Reference:

QUESTION 7
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: (none)
Explanation

Explanation/Reference:

QUESTION 8

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: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
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: (none)
Explanation

Explanation/Reference:

QUESTION 10
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: (none)
Explanation

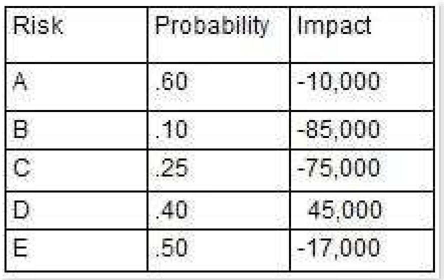
Explanation/Reference:

QUESTION 11
SIMULATION
Fill in the blank with an appropriate phrase.________ models address specifications, requirements, and design, verification and validation, and maintenance activities.

Correct Answer: Life cycle
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
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: (none)

Explanation

Explanation/Reference:

QUESTION 13
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: BCDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
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: (none)
Explanation

Explanation/Reference:

QUESTION 15

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: (none)
Explanation

Explanation/Reference:

QUESTION 16
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: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
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: (none)
Explanation

Explanation/Reference:

QUESTION 18
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: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
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: (none)
Explanation

Explanation/Reference:

QUESTION 20
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: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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 22
Which of the following analysis provides a foundation for measuring investment of time, money and human resources required to achieve a particular outcome?

GRATIS EXAM
Free Practice Exams

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
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 24
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 25
You work as a security manager for SoftTech Inc. You are conducting a security awareness campaign for your employees. One of the employees of your organization asks you the purpose of the security awareness, training and education program. What will be your answer?

A. It improves the possibility for career advancement of the IT staff.
B. It improves the security of vendor relations.
C. It improves the performance of a company's intranet.
D. It improves awareness of the need to protect system resources.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
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 27
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 28
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 29
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 30
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 31
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 32
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 33
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 34
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 35
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 36
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 37
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 38
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 39
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 40
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 41
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 42
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 43
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 44
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 45
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 46
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 47
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 48
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 49
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 50
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 51
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 52
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 53
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 54
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 55
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 56
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 57
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 58
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 59
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 60
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 61
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 62
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 63
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 64

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: (none)
Explanation

Explanation/Reference:

QUESTION 65
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: (none)
Explanation

Explanation/Reference:

QUESTION 66
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: BD

Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
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: (none)
Explanation

Explanation/Reference:

QUESTION 68
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: (none)
Explanation

Explanation/Reference:

QUESTION 69
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: (none)
Explanation

Explanation/Reference:

QUESTION 70
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

GRATIS EXAM
Free Practice Exams
https://www.gratisexam.com/

Correct Answer: Patch management
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
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: (none)
Explanation

Explanation/Reference:

QUESTION 72
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: (none)
Explanation

Explanation/Reference:

QUESTION 73
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: (none)
Explanation

Explanation/Reference:

QUESTION 74
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: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
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: (none)
Explanation

Explanation/Reference:

QUESTION 76
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 77
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 78
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 79
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 80
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 81
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 82
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 83
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 84
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 85
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 86
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 87
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 88
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 89
How many change control systems are there in project management?

A. 3
B. 4
C. 2
D. 1

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
In which of the following phases of the SDLC does the software and other components of the system faithfully incorporate the design specifications and provide proper documentation and training?

A. Programming and training
B. Evaluation and acceptance
C. Initiation
D. Design

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Which of the following signatures watches for the connection attempts to well-known, frequently attacked ports?

A. Port signatures
B. Digital signatures
C. Header condition signatures
D. String signatures

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Configuration Management (CM) is an Information Technology Infrastructure Library (ITIL) IT Service Management (ITSM) process. Configuration Management is used for which of the following? 1.To account for all IT assets 2.To provide precise information support to other ITIL disciplines 3.To provide a solid base only for Incident and Problem Management 4.To verify configuration records and correct any exceptions

A. 1, 3, and 4 only
B. 2 and 4 only
C. 1, 2, and 4 only
D. 2, 3, and 4 only

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Which of the following protocols are used to provide secure communication between a client and a server over the Internet? Each correct answer represents a part of the solution. Choose two.

A. TLS
B. HTTP
C. SNMP

D. SSL

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
How can you calculate the Annualized Loss Expectancy (ALE) that may occur due to a threat?

A. Single Loss Expectancy (SLE)/ Exposure Factor (EF)
B. Asset Value X Exposure Factor (EF)
C. Exposure Factor (EF)/Single Loss Expectancy (SLE)
D. Single Loss Expectancy (SLE) X Annualized Rate of Occurrence (ARO)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Which of the following rate systems of the Orange book has no security controls?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which of the following documents is described in the statement below? "It is developed along with all processes of the risk management. It contains the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning."

A. Risk register
B. Risk management plan
C. Quality management plan
D. Project charter

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Which of the following authentication protocols provides support for a wide range of authentication methods, such as smart cards and certificates?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which of the following test methods has the objective to test the IT system from the viewpoint of a threat-source and to identify potential failures in the IT system protection schemes?

A. Penetration testing
B. On-site interviews
C. Security Test and Evaluation (ST&E)
D. Automated vulnerability scanning tool

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following statements reflect the 'Code of Ethics Preamble' in the '(ISC)2 Code of Ethics'? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Which of the following options is an approach to restricting system access to authorized users?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
You are the project manager for TTX project. You have to procure some electronics gadgets for the project. A relative of yours is in the retail business of those gadgets. He approaches you for your favor to get the order. This is the situation of ____.

A. Conflict of interest
B. Bribery
C. Illegal practice
D. Irresponsible practice

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
What course of action can be taken by a party if the current negotiations fail and an agreement cannot be reached?

A. ZOPA
B. PON
C. Bias
D. BATNA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
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 104
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 105
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 106
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 107
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 108
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 109
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 110
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 111
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 112
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 113
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 114
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 115
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 116
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 117
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 118
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 119
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 120
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 121
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 122
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 123
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 124
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 125
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 126
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 127
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 128
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 129
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: (none)
Explanation

Explanation/Reference:

QUESTION 130
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: (none)
Explanation

Explanation/Reference:

QUESTION 131
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: (none)
Explanation

Explanation/Reference:

QUESTION 132
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: (none)
Explanation

Explanation/Reference:

QUESTION 133
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: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
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: (none)
Explanation

Explanation/Reference:

QUESTION 135
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: (none)
Explanation

Explanation/Reference:

GRATISEXAM
Free Practice Exams
https://www.gratisexam.com/