CISSP-ISSMP

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

CISSP-ISSMP

https://www.gratisexam.com/

Exam A

QUESTION 1
Which of the following fields of management focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following are the ways of sending secure e-mail messages over the Internet? Each correct answer represents a complete solution. Choose two.

A. TLS
B. PGP
C. S/MIME
D. IPSec

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
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: (none)
Explanation

Explanation/Reference:

QUESTION 4
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: (none)
Explanation

Explanation/Reference:

QUESTION 5
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: (none)
Explanation

Explanation/Reference:

QUESTION 6
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: (none)
Explanation

Explanation/Reference:

QUESTION 7
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: (none)
Explanation

Explanation/Reference:

QUESTION 8
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 9
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 10
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: (none)
Explanation

Explanation/Reference:

QUESTION 11
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 12
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 13
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 14
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 15
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 16
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 17
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: (none)
Explanation

Explanation/Reference:

QUESTION 18
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 19
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 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
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 22
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 23
You are the project manager of the HJK project for your organization. You and the project team have created risk responses for many of the risk events in the project. A teaming agreement is an example of what risk response?

A. Mitigation
B. Sharing
C. Acceptance
D. Transference

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which of the following steps is the initial step in developing an information security strategy?

A. Perform a technical vulnerabilities assessment.
B. Assess the current levels of security awareness.

C. Perform a business impact analysis.
D. Analyze the current business strategy.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Against which of the following does SSH provide protection? Each correct answer represents a complete solution. Choose two.

A. IP spoofing
B. Broadcast storm
C. Password sniffing
D. DoS attack

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
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 27
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 28
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 29
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 30
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 31
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 32
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 33
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 34
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 35
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 36
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 37
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 38
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 39
Which of the following statements about Due Care policy is true?

A. It is a method used to authenticate users on a network.
B. It is a method for securing database servers.

C. It identifies the level of confidentiality of information.
D. It provides information about new viruses.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Part of your change management plan details what should happen in the change control system for your project. Theresa, a junior project manager, asks what the configuration management activities are for scope changes. You tell her that all of the following are valid configuration management activities except for which one?

A. Configuration Verification and Auditing
B. Configuration Item Costing
C. Configuration Identification
D. Configuration Status Accounting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Which of the following is a documentation of guidelines that are used to create archival copies of important data?

A. User policy
B. Security policy
C. Audit policy
D. Backup policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which of the following sections come under the ISO/IEC 27002 standard?

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

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
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 44
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 45
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 46
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 47
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 48
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 49
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 50
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 51
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 52
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 53
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 54
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 55
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 56
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 57

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 58
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 59
Which of the following representatives of incident response team takes forensic backups of the systems that are the focus of the incident?

A. Legal representative
B. Technical representative
C. Lead investigator
D. Information security representative

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 60
A Web-based credit card company had collected financial and personal details of Mark before issuing him a credit card. The company has now provided Mark's financial and personal details to another company. Which of the following Internet laws has the credit card issuing company violated?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Which of the following statements are true about security risks? Each correct answer represents a complete solution. Choose three.

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

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which of the following BCP teams provides clerical support to the other teams and serves as a message center for the user-recovery site?

A. Security team

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following architecturally related vulnerabilities is a hardware or software mechanism, which was installed to permit system maintenance and to bypass the system's security protections?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
You have created a team of HR Managers and Project Managers for Blue Well Inc. The team will concentrate on hiring some new employees for the company and improving the organization's overall security by turning employees among numerous job positions. Which of the following steps will you perform to accomplish the task?

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

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 65
You work as a project manager for SoftTech Inc. A threat with a dollar value of $150,000 is expected to happen in your project and the frequency of threat occurrence per year is 0.001. What will be the annualized loss expectancy in your project?

A. $180.25
B. $150
C. $100
D. $120

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which of the following are the responsibilities of the owner with regard to data in an information classification program? Each correct answer represents a complete solution. Choose three.

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

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
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 68
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 69
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 70
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 71
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 72
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 73
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 74
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 75
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 76
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 77
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 78
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 79
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 80
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 81
Which of the following terms describes a repudiation of a contract that occurs before the time when performance is due?

A. Expected breach
B. Actual breach
C. Anticipatory breach
D. Nonperforming breach

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Which of the following elements of BCP process includes the areas of plan implementation, plan testing, and ongoing plan maintenance, and also involves defining and documenting the continuity strategy?

A. Business continuity plan development
B. Business impact assessment
C. Scope and plan initiation
D. Plan approval and implementation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which of the following Acts enacted in United States allows the FBI to issue National Security Letters (NSLs) to Internet service providers (ISPs) ordering them to disclose records about their customers?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
You work as a Product manager for Marioiss Inc. You have been tasked to start a project for securing the network of your company. You want to employ configuration management to efficiently manage the procedures of the project. What will be the benefits of employing configuration management for completing this project? Each correct answer represents a complete solution. Choose all that apply.

A. It provides object, orient, decide and act strategy.
B. It provides a live documentation of the project.
C. It provides the risk analysis of project configurations.
D. It provides the versions for network devices.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
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 87
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 88
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 89
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 90
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 91
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 92
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 93
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 94
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 95
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 96
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 97
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 98
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 99
Which of the following plans provides procedures for recovering business operations immediately following a disaster?

A. Disaster recovery plan
B. Business continuity plan
C. Continuity of operation plan

D. Business recovery plan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Which of the following processes is a structured approach to transitioning individuals, teams, and organizations from a current state to a desired future state?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
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: (none)
Explanation

Explanation/Reference:

QUESTION 102
Which of the following is the default port for Secure Shell (SSH)?

A. UDP port 161
B. TCP port 22
C. UDP port 138
D. TCP port 443

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
You work as a security manager for SoftTech Inc. You along with your team are doing the disaster recovery for your project. Which of the following steps are performed by you for secure recovery based on the extent of the disaster and the organization's recovery ability? Each correct answer represents a part of the solution. Choose three.

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

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
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 105
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 106
Which of the following 'Code of Ethics Canons' of the '(ISC)2 Code of Ethics' states to act honorably, honestly, justly, responsibly and legally?

A. Second Code of Ethics Canons
B. Fourth Code of Ethics Canons
C. First Code of Ethics Canons
D. Third Code of Ethics Canons

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
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 108
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 109
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: (none)
Explanation

Explanation/Reference:

QUESTION 110
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: (none)
Explanation

Explanation/Reference:

QUESTION 111
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 112
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 113
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: (none)
Explanation

Explanation/Reference:

QUESTION 114
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 115
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 116
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:

QUESTION 117
Sarah has created a site on which she publishes a copyrighted material. She is ignorant that she is infringing copyright. Is she guilty under copyright laws?

A. No
B. Yes

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
Which of the following can be done over telephone lines, e-mail, instant messaging, and any other method of communication considered private.

A. Shielding
B. Spoofing
C. Eavesdropping
D. Packaging

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
In which of the following mechanisms does an authority, within limitations, specify what objects can be accessed by a subject?

A. Role-Based Access Control
B. Discretionary Access Control
C. Task-based Access Control
D. Mandatory Access Control

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
Which of the following access control models are used in the commercial sector? Each correct answer represents a complete solution. Choose two.

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference: