

Exam Questions CISSP-ISSMP

Information Systems Security Management Professional

<https://www.2passeasy.com/dumps/CISSP-ISSMP/>



NEW 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

Answer: A

NEW 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

Answer: BC

NEW 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

Answer: D

NEW QUESTION 4

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

Answer: D

NEW QUESTION 5

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

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

Answer: C

NEW QUESTION 6

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

Answer: ACD

NEW QUESTION 7

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

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

Answer: A

NEW QUESTION 8

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

Answer: C

NEW QUESTION 9

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

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

Answer: D

NEW QUESTION 10

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

Answer: C

NEW QUESTION 10

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

Answer: D

NEW QUESTION 15

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

- A. Life cycle

Answer: A

NEW QUESTION 20

Which of the following statements about system hardening are true? Each correct answer represents a complete solution. Choose two.

- A. It can be achieved by installing service packs and security updates on a regular basis.
- B. It is used for securing the computer hardware.
- C. It can be achieved by locking the computer room.
- D. It is used for securing an operating system

Answer: AD

NEW QUESTION 22

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

Answer: BCDE

NEW QUESTION 26

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

Answer: A

NEW QUESTION 30

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

Answer: B

NEW QUESTION 33

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

Answer: ABD

NEW QUESTION 38

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

Answer: A

NEW QUESTION 43

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

Answer: C

NEW QUESTION 44

What are the purposes of audit records on an information system? Each correct answer represents a complete solution. Choose two.

- A. Troubleshooting
- B. Investigation
- C. Upgradation
- D. Backup

Answer: AB

NEW QUESTION 45

Which of the following refers to an information security document that is used in the United States Department of Defense (DoD) to describe and accredit networks and systems?

- A. SSAA
- B. FITSAF
- C. FIPS
- D. TCSEC

Answer: A

NEW QUESTION 50

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

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

Answer: C

NEW QUESTION 55

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

Answer: D

NEW QUESTION 58

Your company is covered under a liability insurance policy, which provides various liability coverage for information security risks, including any physical damage of assets, hacking attacks, etc. Which of the following risk management techniques is your company using?

- A. Risk mitigation
- B. Risk transfer
- C. Risk acceptance
- D. Risk avoidance

Answer: B

NEW QUESTION 63

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 resource

Answer: D

NEW QUESTION 67

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

Answer: D

NEW QUESTION 71

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

Answer: ABCEF

NEW QUESTION 74

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

Answer: B

NEW QUESTION 78

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

- A. Perform a technical vulnerabilities assessment.
- B. Assess the current levels of security awareness.
- C. Perform a business impact analysis.
- D. Analyze the current business strateg

Answer: D

NEW QUESTION 81

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

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

Answer: ACD

NEW QUESTION 82

Which of the following contract types is described in the statement below? "This contract type provides no incentive for the contractor to control costs and hence is rarely utilized."

- A. Cost Plus Fixed Fee
- B. Cost Plus Percentage of Cost
- C. Cost Plus Incentive Fee
- D. Cost Plus Award Fee

Answer: B

NEW QUESTION 84

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

Answer: AC

NEW QUESTION 89

What is a stakeholder analysis chart?

- A. It is a matrix that documents stakeholders' threats, perceived threats, and communication needs.
- B. It is a matrix that identifies all of the stakeholders and to whom they must report to.
- C. It is a matrix that documents the stakeholders' requirements, when the requirements were created, and when the fulfillment of the requirements took place..
- D. It is a matrix that identifies who must communicate with who

Answer: A

NEW QUESTION 93

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

Answer: D

NEW QUESTION 98

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

Answer: C

NEW QUESTION 99

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

Answer: B

NEW QUESTION 100

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)

Answer: C

NEW QUESTION 101

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

Answer: C

NEW QUESTION 104

Change Management is used to ensure that standardized methods and procedures are used for efficient handling of all changes. Who decides the category of a change?

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

Answer: C

NEW QUESTION 107

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

Answer: B

NEW QUESTION 111

The goal of Change Management is to ensure that standardized methods and procedures are used for efficient handling of all changes. Which of the following are Change Management terminologies? Each correct answer represents a part of the solution. Choose three.

- A. Request for Change
- B. Service Request Management
- C. Change
- D. Forward Schedule of Changes

Answer: ACD

NEW QUESTION 116

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

Answer: C

NEW QUESTION 118

You are advising a school district on disaster recovery plans. In case a disaster affects the main IT centers for the district they will need to be able to work from an

alternate location. However, budget is an issue. Which of the following is most appropriate for this client?

- A. Cold site
- B. Off site
- C. Hot site
- D. Warm site

Answer: A

NEW QUESTION 121

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

Answer: B

NEW QUESTION 124

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

Answer: B

NEW QUESTION 126

You are documenting your organization's change control procedures for project management. What portion of the change control process oversees features and functions of the product scope?

- A. Configuration management
- B. Product scope management is outside the concerns of the project.
- C. Scope changecontrol system
- D. Project integration management

Answer: A

NEW QUESTION 128

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

Answer: B

NEW QUESTION 130

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

Answer: CD

NEW QUESTION 135

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

Answer: A

NEW QUESTION 139

Which of the following ports is the default port for Layer 2 Tunneling Protocol (L2TP) ?

- A. UDP port 161

- B. TCP port 443
- C. TCP port 110
- D. UDP port 1701

Answer: D

NEW QUESTION 140

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

Answer: ABD

NEW QUESTION 143

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

Answer: C

NEW QUESTION 145

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

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

Answer: B

NEW QUESTION 147

What are the steps related to the vulnerability management program? Each correct answer represents a complete solution. Choose all that apply.

- A. Maintain and Monitor
- B. Organization Vulnerability
- C. Define Policy
- D. Baseline the Environment

Answer: ACD

NEW QUESTION 149

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

Answer: D

NEW QUESTION 151

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

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

Answer: C

NEW QUESTION 155

Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?

- A. Safeguard
- B. Single Loss Expectancy (SLE)
- C. Exposure Factor (EF)

D. Annualized Rate of Occurrence (ARO)

Answer: D

NEW QUESTION 156

Which of the following types of agreement creates a confidential relationship between the parties to protect any type of confidential and proprietary information or a trade secret?

- A. SLA
- B. NDA
- C. Non-price competition
- D. CNC

Answer: B

NEW QUESTION 160

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

- A. 18 U.S.
- B. 1362
- C. 18 U.S.
- D. 1030
- E. 18 U.S.
- F. 1029
- G. 18 U.S.
- H. 2701
- I. 18 U.S.
- J. 2510

Answer: A

NEW QUESTION 164

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

Answer: B

NEW QUESTION 165

Which of the following administrative policy controls is usually associated with government classifications of materials and the clearances of individuals to access those materials?

- A. Separation of Duties
- B. Due Care
- C. Acceptable Use
- D. Need to Know

Answer: D

NEW QUESTION 170

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

Answer: ABCDE

NEW QUESTION 172

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

Answer: C

NEW QUESTION 176

Which of the following needs to be documented to preserve evidences for presentation in court?

- A. Separation of duties
- B. Account lockout policy
- C. Incident response policy
- D. Chain of custody

Answer: D

NEW QUESTION 178

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.

Answer: A

NEW QUESTION 182

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)

Answer: D

NEW QUESTION 185

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

Answer: A

NEW QUESTION 187

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

Answer: A

NEW QUESTION 188

Fill in the blank with the appropriate phrase. _____ is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time.

- A. Configuration status accounting

Answer: A

NEW QUESTION 190

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

Answer: B

NEW QUESTION 191

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

Answer: D

NEW QUESTION 195

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 dependson what the termination clause of the contract stipulates.
- D. No, the ZAS Corporation did not complete all of the wor

Answer: C

NEW QUESTION 199

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. Minimizethe 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 disaste

Answer: ABC

NEW QUESTION 200

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

Answer: B

NEW QUESTION 205

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

Answer: D

NEW QUESTION 208

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

Answer: ABD

NEW QUESTION 212

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

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

Answer: B

NEW QUESTION 216

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

Answer: B

NEW QUESTION 218

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

Answer: C

NEW QUESTION 223

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

Answer: ACD

NEW QUESTION 228

Which of the following methods for identifying appropriate BIA interviewees' includes examining the organizational chart of the enterprise to understand the functional positions?

- A. Organizational chart reviews
- B. Executive management interviews
- C. Overlaying system technology
- D. Organizational process models

Answer: A

NEW QUESTION 232

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

Answer: A

NEW QUESTION 234

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

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

Answer: B

NEW QUESTION 239

Which of the following persons is responsible for testing and verifying whether the security policy is properly implemented, and the derived security solutions are adequate or not?

- A. Data custodian
- B. Auditor
- C. User
- D. Data owner

Answer: B

NEW QUESTION 242

Which of the following are the process steps of OPSEC? Each correct answer represents a part of the solution. Choose all that apply.

- A. Analysis of Vulnerabilities
- B. Display of associated vulnerability components
- C. Assessment of Risk
- D. Identification of Critical Information

Answer: ACD

NEW QUESTION 243

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

Answer: B

NEW QUESTION 245

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

Answer: ABC

NEW QUESTION 247

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 privilege

Answer: A

NEW QUESTION 248

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 resource

Answer: B

NEW QUESTION 253

Fill in the blank with an appropriate phrase. _____ is a branch of forensic science pertaining to legal evidence found in computers and digital storage media.

- A. Computer forensics

Answer: A

NEW QUESTION 258

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

Answer: D

NEW QUESTION 259

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

Answer: D

NEW QUESTION 264

How many change control systems are there in project management?

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

Answer: B

NEW QUESTION 265

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

Answer: A

NEW QUESTION 267

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

Answer: A

NEW QUESTION 272

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

Answer: AD

NEW QUESTION 276

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

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

Answer: B

NEW QUESTION 278

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

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

Answer: C

NEW QUESTION 279

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

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

Answer: D

NEW QUESTION 284

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

Answer: C

NEW QUESTION 286

Which of the following is generally practiced by the police or any other recognized governmental authority?

- A. Phishing
- B. Wiretapping
- C. SMB signing
- D. Spoofing

Answer: B

NEW QUESTION 288

Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?

- A. Safeguard
- B. Single Loss Expectancy (SLE)
- C. Exposure Factor (EF)
- D. Annualized Rate of Occurrence (ARO)

Answer: D

NEW QUESTION 290

Which of the following statements is related with the second law of OPSEC?

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

Answer: B

NEW QUESTION 295

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

Answer: A

NEW QUESTION 298

Fill in the blank with an appropriate phrase. An is an intensive application of the OPSEC process to an existing operation or activity by a multidiscipline team of experts.

- A. OPSEC assessment

Answer: A

NEW QUESTION 301

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

Answer: A

NEW QUESTION 305

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 device

Answer: BD

NEW QUESTION 306

Your company suspects an employee of sending unauthorized emails to competitors. These emails are alleged to contain confidential company data. 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

Answer: A

NEW QUESTION 310

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

Answer: BDEF

NEW QUESTION 312

Which of the following is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known, but by which a business can obtain an economic advantage over its competitors?

- A. Utility model
- B. Cookie
- C. Copyright
- D. Trade secret

Answer: D

NEW QUESTION 314

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

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

Answer: A

NEW QUESTION 316

John works as a security manager for Soft Tech Inc. He is working with his team on the disaster recovery management plan. One of his team members has a doubt related to the most cost-effective DRP testing plan. According to you, which of the following disaster recovery testing plans is the most cost-effective and efficient way to identify areas of overlap in the plan before conducting more demanding training exercises?

- A. Full-scale exercise
- B. Walk-through drill
- C. Evacuation drill
- D. Structured walk-through test

Answer: D

NEW QUESTION 318

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

Answer: ABCD

NEW QUESTION 322

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

Answer: A

NEW QUESTION 325

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.

Answer: ABCD

NEW QUESTION 329

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.
- B. 1362
- C. 18 U.S.
- D. 1030
- E. 18 U.S.
- F. 2701
- G. 18 U.S.
- H. 2510

Answer: B

NEW QUESTION 330

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 warm 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.

Answer: AD

NEW QUESTION 334

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. Videosurveillance on all areas with computers.
- B. Use laptop locks.
- C. Appoint a security guard.
- D. Smart card access to all areas with computers.

Answer: B

NEW QUESTION 338

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

Answer: B

NEW QUESTION 340

In which of the following contract types, the seller is reimbursed for all allowable costs for performing the contract work and receives a fixed fee payment which is calculated as a percentage of the initial estimated project costs?

- A. Firm Fixed Price Contracts
- B. Cost Plus Fixed Fee Contracts
- C. Fixed Price Incentive Fee Contracts
- D. Cost Plus Incentive Fee Contracts

Answer: B

NEW QUESTION 342

Which of the following types of cyber stalking damage the reputation of their victim and turn other people against them by setting up their own Websites, blogs or user pages for this purpose?

- A. Encouraging others to harass the victim
- B. False accusations
- C. Attempts to gather information about the victim
- D. False victimization

Answer: B

NEW QUESTION 346

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

Answer: C

NEW QUESTION 351

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

Answer: C

NEW QUESTION 354

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

Answer: B

NEW QUESTION 359

Which of the following is used to back up forensic evidences or data folders from the network or locally attached hard disk drives?

- A. WinHex
- B. Vedit
- C. Device Seizure
- D. FAR system

Answer: D

NEW QUESTION 363

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

Answer: ACD

NEW QUESTION 367

Management has asked you to perform a risk audit and report back on the results. Bonny, a project team member asks you what a risk audit is. What do you tell Bonny?

- A. A risk audit is a review of all the risks that have yet to occur and what their probability of happening are.
- B. A risk audit is a review of the effectiveness of the risk responses in dealing with identified risks and their root causes, as well as the effectiveness of the risk management process.
- C. A risk audit is a review of all the risk probability and impact for the risks, which are still present in the project but which have not yet occurred.
- D. A risk audit is an audit of all the risks that have occurred in the project and what their true impact on cost and time has been.

Answer: B

NEW QUESTION 372

Which of the following steps are generally followed in computer forensic examinations? Each correct answer represents a complete solution. Choose three.

- A. Acquire
- B. Analyze
- C. Authenticate
- D. Encrypt

Answer: ABC

NEW QUESTION 375

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

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

Answer: A

NEW QUESTION 377

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

Answer: A

NEW QUESTION 380

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

Answer: D

NEW QUESTION 381

Which of the following measurements of an enterprise's security state is the process whereby an organization establishes the parameters within which programs, investments, and acquisitions reach the desired results?

- A. Information sharing
- B. Ethics
- C. Performance measurement
- D. Risk management

Answer: C

NEW QUESTION 385

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

Answer: A

NEW QUESTION 388

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

Answer: C

NEW QUESTION 393

Which of the following sites are similar to the hot site facilities, with the exception that they are completely dedicated, self-developed recovery facilities?

- A. Cold sites
- B. Orange sites
- C. Warm sites
- D. Duplicate processing facilities

Answer: D

NEW QUESTION 395

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

Answer: B

NEW QUESTION 396

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

Answer: B

NEW QUESTION 398

Which of the following laws is defined as the Law of Nations or the legal norms that has developed through the customary exchanges between states over time, whether based on diplomacy or aggression?

- A. Customary
- B. Tort
- C. Criminal
- D. Administrative

Answer: A

NEW QUESTION 403

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

Answer: C

NEW QUESTION 406

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 Initiative (IINI)

Answer: B

NEW QUESTION 408

You work as the project manager for Bluewell Inc. You are working on NGQQ Project for your company. You have completed the risk analysis processes for the

risk events. You and the project team have created risk responses for most of the identified project risks. Which of the following risk response planning techniques will you use to shift the impact of a threat to a third party, together with the responses?

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

Answer: D

NEW QUESTION 409

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

- A. Model

Answer: A

NEW QUESTION 414

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

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

Answer: B

NEW QUESTION 415

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

Answer: B

NEW QUESTION 420

Which of the following models uses a directed graph to specify the rights that a subject can transfer to an object or that a subject can take from another subject?

- A. Take-Grant Protection Model
- B. Bell-LaPadula Model
- C. Biba Integrity Model
- D. Access Matrix

Answer: A

NEW QUESTION 421

Which of the following concepts represent the three fundamental principles of information security? Each correct answer represents a complete solution. Choose three.

- A. Confidentiality
- B. Integrity
- C. Availability
- D. Privacy

Answer: ABC

NEW QUESTION 426

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

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

Answer: C

NEW QUESTION 430

You work as the Senior Project manager in Dotcoiss Inc. Your company has started a software project using configuration management and has completed 70% of it. You need to ensure that the network infrastructure devices and networking standards used in this project are installed in accordance with the requirements of its detailed project design documentation. Which of the following procedures will you employ to accomplish the task?

- A. Configuration identification
- B. Physical configuration audit
- C. Configuration control
- D. Functional configuration audit

Answer: B

NEW QUESTION 431

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

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

Answer: B

NEW QUESTION 434

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

Answer: BD

NEW QUESTION 438

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CISSP-ISSMP Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CISSP-ISSMP Product From:

<https://www.2passeasy.com/dumps/CISSP-ISSMP/>

Money Back Guarantee

CISSP-ISSMP Practice Exam Features:

- * CISSP-ISSMP Questions and Answers Updated Frequently
- * CISSP-ISSMP Practice Questions Verified by Expert Senior Certified Staff
- * CISSP-ISSMP Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CISSP-ISSMP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year