

ISC2

Exam Questions CISSP-ISSMP

Information Systems Security Management Professional



NEW QUESTION 1

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

Answer: D

NEW QUESTION 2

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

Answer: B

NEW QUESTION 3

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

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

Answer: ABC

NEW QUESTION 4

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 5

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

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

Answer: C

NEW QUESTION 6

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

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

Answer: D

NEW QUESTION 7

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

Answer: BCD

NEW QUESTION 8

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

Answer: B

NEW QUESTION 9

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 10

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 10

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

Answer: C

NEW QUESTION 14

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 16

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 17

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 19

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 23

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 24

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 29

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 30

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 35

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 38

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 40

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 42

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

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

Answer: D

NEW QUESTION 44

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

Answer: C

NEW QUESTION 45

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

Answer: D

NEW QUESTION 49

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 52

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 53

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 56

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 60

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 64

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 65

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.

Answer: B

NEW QUESTION 67

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 69

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. Baselineing
- D. Compliance checking

Answer: A

NEW QUESTION 71

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 76

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 78

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

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

Answer: BD

NEW QUESTION 80

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

Answer: A

NEW QUESTION 83

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 88

You are working as a project manager in your organization. You are nearing the final stages of project execution and looking towards the final risk monitoring and controlling activities. For your project archives, which one of the following is an output of risk monitoring and control?

- A. Quantitative risk analysis
- B. Qualitative risk analysis
- C. Requested changes
- D. Risk audits

Answer: C

NEW QUESTION 92

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

- A. Data classification

Answer: A

NEW QUESTION 93

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 96

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 101

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

Answer: AB

NEW QUESTION 102

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

Answer: ACD

NEW QUESTION 104

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 vulnerabilit

Answer: ACD

NEW QUESTION 109

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

Answer: C

NEW QUESTION 112

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 115

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 117

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 119

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 124

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. Correctiveaction

Answer: D

NEW QUESTION 125

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 130

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

Answer: C

NEW QUESTION 134

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

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

Answer: A

NEW QUESTION 139

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

Answer: A

NEW QUESTION 142

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

Answer: A

NEW QUESTION 144

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 149

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

Answer: A

NEW QUESTION 152

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 154

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 155

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 158

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 161

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 163

You 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 164

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 168

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 173

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 177

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 182

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

Answer: C

NEW QUESTION 185

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

Answer: C

NEW QUESTION 189

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 190

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 191

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 192

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 196

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 198

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 201

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

- A. Model

Answer: A

NEW QUESTION 205

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

Answer: B

NEW QUESTION 208

An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

- A. Network security policy
- B. Backup policy
- C. Privacy policy
- D. User password policy

Answer: C

NEW QUESTION 213

Which of the following plans is designed to protect critical business processes from natural or man-made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes?

- A. Businesscontinuity plan
- B. Crisis communication plan
- C. Contingency plan
- D. Disaster recovery plan

Answer: A

NEW QUESTION 218

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 221

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 224

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 228

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The CISSP-ISSMP Practice Test Here](#)