

ISC2

Exam Questions ISSMP

Information Systems Security Management Professional



NEW QUESTION 1

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

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

Answer: A

NEW QUESTION 2

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 3

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 4

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 5

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 6

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 7

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 8

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 9

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 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. A teaming agreement is an example of what risk response?

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

Answer: B

NEW QUESTION 10

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 11

Ned is the program manager for his organization and he's considering some new materials for his program. He and his team have never worked with these materials before and he wants to ask the vendor for some additional information, a demon, and even some samples. What type of a document should Ned send to the vendor?

- A. IFB
- B. RFQ
- C. RFP
- D. RFI

Answer: D

NEW QUESTION 15

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 16

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 20

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 21

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 23

Which of the following is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention?

- A. Patent
- B. Utility model
- C. Snooping
- D. Copyright

Answer: A

NEW QUESTION 28

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 31

Which of the following issues are addressed by the change control phase in the maintenance phase of the life cycle models? Each correct answer represents a complete solution. Choose all that apply.

- A. Performing quality control
- B. Recreating and analyzing the problem
- C. Developing the changes and corresponding tests
- D. Establishing the priorities of requests

Answer: ABC

NEW QUESTION 34

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 35

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 38

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 43

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 45

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 47

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 48

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 50

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 54

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 56

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

Answer: ACD

NEW QUESTION 57

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 59

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 62

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 66

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 69

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

Answer: A

NEW QUESTION 70

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 74

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

Answer: D

NEW QUESTION 75

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 78

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 79

How many change control systems are there in project management?

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

Answer: B

NEW QUESTION 83

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 86

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 90

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 91

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 93

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 94

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 96

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 101

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 102

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 106

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

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

Answer: A

NEW QUESTION 110

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 114

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 117

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 122

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 125

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

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

Answer: B

NEW QUESTION 127

Which of the following methods can be helpful to eliminate social engineering threat? Each correct answer represents a complete solution. Choose three.

- A. Password policies
- B. Vulnerability assessments
- C. Data encryption
- D. Data classification

Answer: ABD

NEW QUESTION 132

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

Answer: A

NEW QUESTION 136

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 138

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 141

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 143

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

- A. Model

Answer: A

NEW QUESTION 147

Which of the following are known as the three laws of OPSEC? Each correct answer represents a part of the solution. Choose three.

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

Answer: ABC

NEW QUESTION 149

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. Business continuity plan
- B. Crisis communication plan
- C. Contingency plan
- D. Disaster recovery plan

Answer: A

NEW QUESTION 154

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 158

.....

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

ISSMP Practice Exam Features:

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

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