

# ISC2

## Exam Questions ISSMP

Information Systems Security Management Professional



#### NEW QUESTION 1

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 2

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 3

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 4

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 5

Which of the following characteristics are described by the DIAP Information Readiness Assessment function? Each correct answer represents a complete solution. Choose all that apply.

- A. It performs vulnerability/threat analysis assessment.
- B. It identifies and generates IA requirements.
- C. It provides data needed to accurately assess IA readiness.
- D. It provides for entry and storage of individual system dat

**Answer: ABC**

#### NEW QUESTION 6

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 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**

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 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 10**

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 12**

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 14**

You are responsible for network and information security at a metropolitan police station. The most important concern is that unauthorized parties are not able to access data. What is this called?

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

**Answer:** D

**NEW QUESTION 16**

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 19

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 22

Which of the following acts is a specialized privacy bill that affects any educational institution to accept any form of funding from the federal government?

- A. HIPAA
- B. COPPA
- C. FERPA
- D. GLBA

**Answer: C**

#### NEW QUESTION 24

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 29

In which of the following SDLC phases is the system's security features configured and enabled, the system is tested and installed or fielded, and the system is authorized for processing?

- A. Initiation Phase
- B. Development/Acquisition Phase
- C. Implementation Phase
- D. Operation/Maintenance Phase

**Answer: C**

#### NEW QUESTION 30

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 34

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 39

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 42**

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 44**

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 46**

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 47**

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 51**

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 56**

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 61**

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 63**

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 68**

You are an Incident manager in Orangesect.Inc. You have been tasked to set up a new extension of your enterprise. The networking, to be done in the new extension, requires different types of cables and an appropriate policy that will be decided by you. Which of the following stages in the Incident handling process involves your decision making?

- A. Preparation
- B. Eradication
- C. Identification
- D. Containment

**Answer:** A

**NEW QUESTION 72**

Which of the following BCP teams handles financial arrangement, public relations, and media inquiries in the time of disaster recovery?

- A. Software team
- B. Off-site storage team
- C. Applications team
- D. Emergency-management team

**Answer:** D

**NEW QUESTION 76**

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 81**

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 84**

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 86**

You work as a Web Administrator for Perfect World Inc. The company is planning to host an E-commerce Web site. You are required to design a security plan for it. Client computers with different operating systems will access the Web server. How will you configure the Web server so that it is secure and only authenticated users are able to access it? Each correct answer represents a part of the solution. Choose two.

- A. Use encrypted authentication.
- B. Use the SSL protocol.
- C. Use the EAP protocol.
- D. Use Basic authenticatio

**Answer:** AB

**NEW QUESTION 87**

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 90

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 95

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 97

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 100

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 directio

**Answer:** D

#### NEW QUESTION 104

How many change control systems are there in project management?

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

**Answer:** B

#### NEW QUESTION 108

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 111**

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 113**

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

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

**Answer: AB**

**NEW QUESTION 118**

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

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

**Answer: C**

**NEW QUESTION 119**

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 122**

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 126**

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 128**

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 131**

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 132**

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 135**

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 137**

Which of the following is the default port for Simple Network Management Protocol (SNMP)?

- A. TCP port 80
- B. TCP port 25
- C. UDP port 161
- D. TCP port 110

**Answer:** C

**NEW QUESTION 138**

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

- A. Determining what level of classification the information requires
- B. Running regular backups and routinely testing the validity of the backup data
- C. Controlling access, adding and removing privileges for individual users
- D. Performing data restoration from the backups when necessary

**Answer:** BCD

**NEW QUESTION 140**

Which of the following statements about Hypertext Transfer Protocol Secure (HTTPS) are true? Each correct answer represents a complete solution. Choose two.

- A. It uses TCP port 80 as the default port.
- B. It is a protocol used in the Universal Resource Locator (URL) address line to connect to a secure site.
- C. It uses TCP port 443 as the default port.
- D. It is a protocol used to provide security for a database server in an internal network

**Answer:** BC

**NEW QUESTION 141**

John is a black hat hacker. FBI arrested him while performing some email scams. Under which of the following US laws will John be charged?

- A. 18 U.S.C. 1362
- B. 18 U.S.C. 1030
- C. 18 U.S.C. 2701
- D. 18 U.S.C. 2510

**Answer:** B

**NEW QUESTION 142**

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 145**

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 146**

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 150**

Which of the following plans provides procedures for recovering business operations immediately following a disaster?

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

**Answer: D**

**NEW QUESTION 152**

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 155**

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 160**

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 165**

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 166**

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 167**

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 170**

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 174**

.....

## **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](#)**