

## Exam Questions CISSP-ISSMP

Information Systems Security Management Professional

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



#### 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 protocols is used with a tunneling protocol to provide security?

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

**Answer:** C

#### NEW QUESTION 3

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 4

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 5

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 6

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 7

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 8

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 9

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 10

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 10

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 15

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 18

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 23

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 26**

Which of the following roles is used to ensure that the confidentiality, integrity, and availability of the services are maintained to the levels approved on the Service Level Agreement (SLA)?

- A. The Service Level Manager
- B. The Configuration Manager
- C. The IT Security Manager
- D. The Change Manager

**Answer:** C

**NEW QUESTION 30**

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 32**

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 35**

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 39**

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

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

**Answer:** BCD

**NEW QUESTION 44**

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 48**

Fill in the blank with an appropriate phrase. \_\_\_\_\_ is the process of using a strategy and plan of what patches should be applied to which systems at a specified time.  
Correct

- A. Patch management

**Answer:** A

#### NEW QUESTION 51

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 53

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 dat

**Answer:** ABC

#### NEW QUESTION 54

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 59

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 63

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 67

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 71

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 75

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

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

**Answer:** C

#### NEW QUESTION 78

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 79

You company suspects an employee of sending unauthorized emails to competitors. These emails are alleged to contain confidential company dat a. 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 activitie

**Answer:** A

#### NEW QUESTION 82

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 87

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 90

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 91

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 93

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 97

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 99

NIST Special Publication 800-50 is a security awareness program. It is designed for those people who are currently working in the information technology field and want information on security policies. Which of the following are some of its critical steps? Each correct answer represents a complete solution. Choose two.

- A. Awareness and Training Material Effectiveness
- B. Awareness and Training Material Development
- C. Awareness and Training Material Implementation
- D. Awareness and Training Program Design

**Answer:** BD

#### NEW QUESTION 104

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 108

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 113

Which of the following are examples of administrative controls that involve all levels of employees within an organization and determine which users have access to what resources and information? Each correct answer represents a complete solution. Choose three.

- A. Employee registration and accounting
- B. Disaster preparedness and recovery plans
- C. Network authentication
- D. Training and awareness
- E. Encryption

**Answer:** ABD

#### NEW QUESTION 118

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 120

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 123

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 125

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 130

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 133

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 135

.....



## 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