ISC2

Exam Questions CISSP-ISSMP

Information Systems Security Management Professional

NEW QUESTION 1
Which of the following fields of management focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life?

A. Configuration management
B. Risk management
C. Procurement management
D. Change management

Answer: A

NEW QUESTION 2
Which of the following are the ways of sending secure e-mail messages over the Internet? Each correct answer represents a complete solution. Choose two.

A. TLS
B. PGP
C. S/MIME
D. IPSec

Answer: BC

NEW QUESTION 3
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 4
Which of the following recovery plans includes specific strategies and actions to deal with specific variances to assumptions resulting in a particular security problem, emergency, or state of affairs?

A. Business continuity plan
B. Disaster recovery plan
C. Continuity of Operations Plan
D. Contingency plan

Answer: D

NEW QUESTION 5
Which of the following protocols is used with a tunneling protocol to provide security?

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

Answer: C

NEW QUESTION 6
Which of the following 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 7
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 8

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 9
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 10
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 10
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 15
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 16
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 orprocesses.
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 17
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 22
Which of the following response teams aims to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large?

A. CSIRT
B. CERT
C. FIRST
D. FedCIRC

Answer: C

NEW QUESTION 25
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 28
Which of the following is the correct order of digital investigations Standard Operating Procedure (SOP)?

A. Initial analysis, request for service, data collection, data reporting, data analysis
B. Initial analysis, request for service, data collection, data analysis, data reporting
C. Request for service, initial analysis, data collection, data analysis, data reporting
D. Request for service, initial analysis, data collection, data reporting, data analysis

Answer: C

NEW QUESTION 31
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 36
You are documenting your organization's change control procedures for project management. What portion of the change control process oversees features and functions of the product scope?

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

Answer: A

NEW QUESTION 41
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 43
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 45

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 50
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. Baselining
D. Compliance checking

Answer: A

NEW QUESTION 54
Which of the following needs to be documented to preserve evidences for presentation in court?

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

Answer: D

NEW QUESTION 59
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 61
Which of the following recovery plans includes specific strategies and actions to deal with specific variances to assumptions resulting in a particular security problem, emergency, or state of affairs?

A. Disaster recovery plan
B. Contingency plan
C. Continuity of Operations Plan
D. Business continuity plan

Answer: B

NEW QUESTION 65
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 67
Which of the following are examples of physical controls used to prevent unauthorized access to sensitive materials?

A. Thermal alarm systems
B. Closed circuit cameras
C. Encryption
D. Security Guards

Answer: ABD

NEW QUESTION 70
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 72
Which of the following laws enacted in United States makes it illegal for an Internet Service Provider (ISP) to allow child pornography to exist on Web sites?

A. Child Pornography Prevention Act (CPPA)
B. USA PATRIOT Act
C. Prosecutorial Remedies and Tools Against the Exploitation of Children Today Act (PROTECT Act)
D. Sexual Predators Act

Answer: D

NEW QUESTION 77
Which of the following methods for identifying appropriate BIA interviewees' includes examining the organizational chart of the enterprise to understand the functional positions?

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

Answer: A

NEW QUESTION 81
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 85
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 89
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 93
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 94
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 97
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 98
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 102
Which of the following is a variant with regard to Configuration Management?

A. A CI thathas 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 versio

Answer: C

NEW QUESTION 105
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 110
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 112
Which of the following is the default port for Secure Shell (SSH)?

A. UDP port 161
B. TCP port 22
C. UDP port 138
D. TCP port 443

Answer: B

NEW QUESTION 115
You work as a security manager for SoftTech Inc. You are conducting a security awareness campaign for your employees. Which of the following ideas will you consider the best when
conducting a security awareness campaign?

A. Target system administrators and the help desk.
B. Provide technical details on exploits.
C. Provide customizedmessages for different groups.
D. Target senior managers and business process owner

Answer: C

NEW QUESTION 116
Which of the following processes provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and the security posture of a system or site?

A. NSA-IAM
B. DITSCAP
C. ASSET
D. NIACAP

Answer: D

NEW QUESTION 121
Fill in the blank with an appropriate word. are used in information security to formalize security policies.

A. Model

Answer: A

NEW QUESTION 125
In which of the following alternative processing sites is the backup facility maintained in a constant order, with a full complement of servers, workstations, and communication links ready to assume the primary operations responsibility?

A. Mobile Site
B. Cold Site
C. Warm Site
D. Hot Site

Answer: D

NEW QUESTION 129
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 132
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 133
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 138
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 139
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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