ISC.Premium.CISSP-ISSMP.by.VCEplus.218q

Number: CISSP-ISSMP VCEplus
Passing Score: 800
Time Limit: 120 min
File Version: 4.5

Exam Code: CISSP-ISSMP
Exam Name: Information Systems Security Management Professional
Certification Provider: ISC
Corresponding Certifications: CISSP Concentrations, CISSP-ISSMP
Website: www.vceplus.com
Free Exam: https://vceplus.com/exam-cissp-issmp/

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
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

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following protocols is used with a tunneling protocol to provide security?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
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

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
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 data.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13

Joseph works as a Software Developer for Web Tech Inc. He wants to protect the algorithms and the techniques of programming that he uses in developing an application. Which of the following laws are used to protect a part of software?

A. Code Security law
B. Trademark laws
C. Copyright laws
D. Patent laws

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Which of the following is the best method to stop vulnerability attacks on a Web server?

A. Using strong passwords
B. Configuring a firewall
C. Implementing the latest virus scanner
D. Installing service packs and updates

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which of the following security models dictates that subjects can only access objects through applications?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
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

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

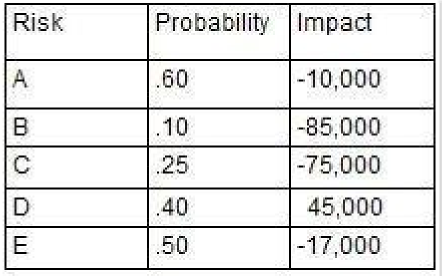
QUESTION 22
SIMULATION Fill in the blank with an appropriate phrase.________ models address specifications, requirements, and design, verification and validation, and maintenance activities.

A. Life cycle

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
You are the project manager of the GHE Project. You have identified the following risks with the characteristics as shown in the following figure:



Risk	Probability	Impact
A	.60	-10,000
B	.10	-85,000
C	.25	-75,000
D	.40	45,000
E	.50	-17,000

How much capital should the project set aside for the risk contingency reserve?

A. $142,000
B. $232,000
C. $41,750
D. $23,750

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
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

Correct Answer: BCDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following processes is described in the statement below? "It is the process of implementing risk response plans, tracking identified risks, monitoring residual risk, identifying new risks, and evaluating risk process effectiveness throughout the project."

A. Monitor and Control Risks
B. Identify Risks
C. Perform Qualitative Risk Analysis
D. Perform Quantitative Risk Analysis

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
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

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following can be prevented by an organization using job rotation and separation of duties policies?

A. Collusion
B. Eavesdropping
C. Buffer overflow
D. Phishing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Peter works as a Computer Hacking Forensic Investigator. He has been called by an organization to conduct a seminar to give necessary information related to sexual harassment within the work place. Peter started with the definition and types of sexual harassment. He then wants to convey that it is important that records of the sexual harassment incidents should be maintained, which helps in further legal prosecution. Which of the following data should be recorded in this documentation? Each correct answer represents a complete solution. Choose all that apply.

A. Names of the victims
B. Location of each incident
C. Nature of harassment
D. Date and time of incident

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference: