ISC2

ISSMP Exam

ISC2 CISSP Information Systems Security Management Professional Exam

Questions & Answers
Demo

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

Explanation:
Configuration management is a field of management that 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.
Configuration Management System is a subsystem of the overall project management system. It is a collection of formal documented procedures used to identify and document the functional and physical characteristics of a product, result, service, or component of the project.
It also controls any changes to such characteristics, and records and reports each change and its implementation status. It includes the documentation, tracking systems, and defined approval levels necessary for authorizing and controlling changes. Audits are performed as part of configuration management to determine if the requirements have been met.
Answer option C is incorrect. The procurement management plan defines more than just the procurement of team members, if needed. It defines how procurements will be planned and executed, and how the organization and the vendor will fulfill the terms of the contract.
Answer option B is incorrect. Risk Management is used to identify, assess, and control risks. It includes analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats.
Answer option D is incorrect. Change Management is used to ensure that standardized methods and procedures are used for efficient handling of all changes.

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: B, C

Explanation:
Pretty Good Privacy (PGP) and Secure Multipurpose Internet Mail Extensions (S/MIME) are two ways of sending secure e-mail messages over the Internet. Both use public key cryptography, where users each possess two keys, a public key for encrypting, and a private key for decrypting messages. Because PGP has evolved from a free distribution, it is more popular than S/MIME.
Answer option A is incorrect. Transport Layer Security (TLS) is an application layer protocol that uses a combination of public and symmetric key processing to encrypt data.
Answer option D is incorrect. Internet Protocol Security (IPSec) is a standard-based protocol that provides the highest level of VPN security. IPSec can encrypt virtually everything above the networking layer. It is used for VPN connections that use the L2TP protocol. It secures both data and password.
IPSec cannot be used with Point-to-Point Tunneling Protocol (PPTP).
Reference: TechNet, Contents: "Ask Us About... Security, October 2000"

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

Answer: D

Explanation:
According to the question, incident response team announced that this was a controlled event not an incident. Incident response team performed the identification step to rectify the incident.
Identification is the first post-attack step in Incident handling process. In this phase of the incident handling process, the Incident Handler determines whether the incident exists or not. An incident is described as an event in a system or network that poses threat to the environment. Identification of an incident becomes more difficult with the increase in the complexity of the attack. The Incident Handler should gather all facts and make decisions on the basis of those facts. Incident Handler needs to identify the following characteristics of an attack before it can be properly processeD.

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

Answer: D

Explanation:
The reciprocal agreements are arrangements between two or more organizations with similar equipment and applications. According to this agreement, organizations provide computer time to each other in the case of an emergency. Theses types of agreements are commonly done between organizations that have unique hardware or software that cannot be maintained at a hot or warm site.
Answer option B is incorrect. A business impact analysis (BIA) is a crisis management and business impact analysis technique that identifies those threats that can impact the business continuity of operations. Such threats can be either natural or man-made. The BIA team should have a clear understanding of the organization, key business processes, and IT resources for assessing the risks associated with continuity. In the BIA team, there should be senior management, IT personnel, and end users to identify all resources that are to be used during normal operations.
Answer option C is incorrect. The duplicate processing facilities work in the same manner as the hot site facilities, with the exception that they are completely dedicated, self-developed recovery facilities. The duplicate facility holds same equipment, operating systems, and applications and might have regularly synchronized data. The examples of the duplicate processing facilities can be the large organizations that have multiple geographic locations.
Answer option A is incorrect. A cold site is a backup site in case disaster has taken place in a data center. This is the least expensive disaster recovery solution, usually having only a single room with no equipment. All equipment is brought to the site after the disaster. It can be on site or off site.

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

Answer: A

Explanation:
Data diddling involves changing data prior to or during input to a computer in an effort to commit fraud. It also refers to the act of intentionally modifying information, programs, or documentations.
Answer option C is incorrect. Eavesdropping is the process of listening in private conversations. It also includes attackers listening in on the network traffic. For example, it can be done over telephone lines (wiretapping), e-mail, instant messaging, and any other method of communication considered private.
Answer option D is incorrect. Spoofing is a technique that makes a transmission appear to have come

from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected.
Answer option B is incorrect. Wiretapping is an act of monitoring telephone and Internet conversations by a third party. It is only legal with prior consent. Legalized wiretapping is generally practiced by the police or any other recognized governmental authority.
Reference: "http://financial-dictionary.thefreedictionary.com/Data+diddling"

Question: 6

Drag and drop the various evidences in the appropriate places.

Drag an item from the item list and drop it on the appropriate spot. To remove an item, drag and drop it anywhere on the window.

DESCRIPTION	CATEGORIES OF EVIDENCES
It is the original or primary evidence rather than a copy or duplicate of the evidence.	Drop Here
It is a copy of the evidence or an oral description of its contents.	Drop Here
It proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses.	Drop Here
It is incontrovertible evidence which overrides all other evidence.	Drop Here

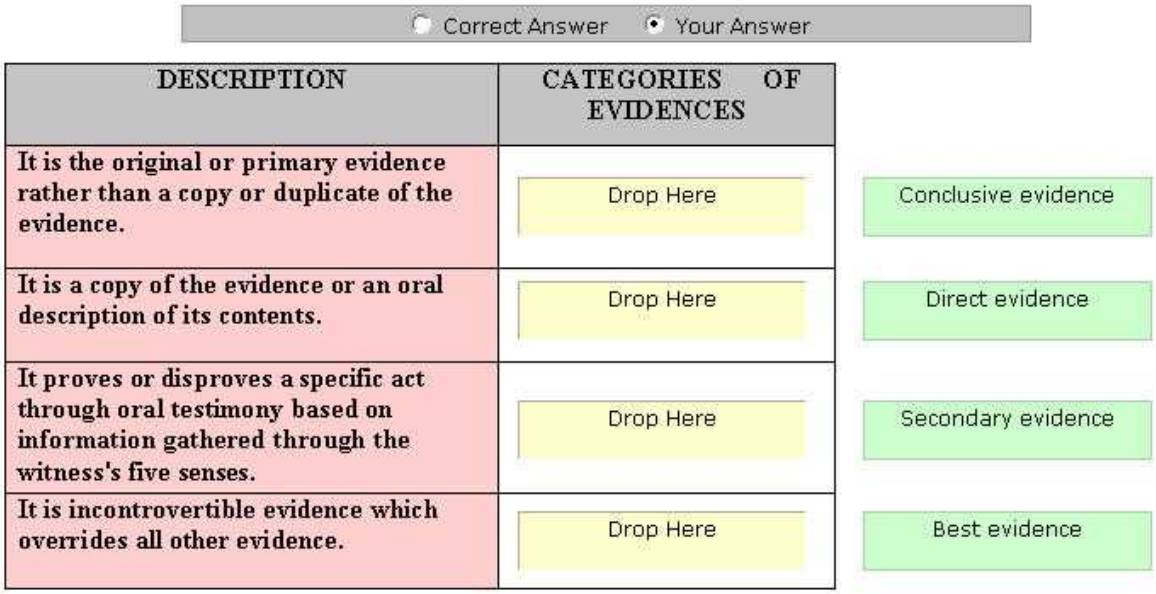
Conclusive evidence

Direct evidence

Secondary evidence

Best evidence

Answer:



Explanation:
The various categories of evidences required in forensics can be divided into a number of categories, depending on its reliability, quality, and completeness. These categories are as follows:
Best evidence: It is the original or primary evidence rather than a copy or duplicate of the evidence.
Secondary evidence: It is a copy of the evidence or an oral description of its contents. It is not as reliable as the best evidence.Direct evidence: It proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses.
Conclusive evidence: It is incontrovertible evidence, which overrides all other evidence.
Opinions: The following are the two types of opinions:
1. Expert: It offers an opinion based on personal expertise and facts.
2. Non expert: It can testify only to facts.Circumstantial evidence:It is the inference of information from other, intermediate, relevant facts.
Hearsay evidence: This evidence is commonly not admissible in court. It is a third-party evidence. Computer-generated records and other business records fall under the category of hearsay evidence because these records cannot be proven accurate and reliable.
Reference: CISM Review Manual 2010, Contents: "Incident Management and Response"

Question: 7

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

Answer: B

Explanation:

The pre-attack phase is the first step for a penetration tester. The pre-attack phase involves reconnaissance or data gathering. It also includes gathering data from Whois, DNS, and network scanning, which help in mapping a target network and provide valuable information regarding the operating system and applications running on the systems. Penetration testing involves locating the IP block and using domain name Whois to find personnel contact information.

Answer option A is incorrect. The attack phase is the most important phase of penetration testing. Different exploitive and responsive hacking tools are used to monitor and test the security of systems and the network. Some of the actions performed in the attack phase are as follows:
Penetrating the perimeter
Escalating privileges
Executing, implanting, and retracting
Answer option C is incorrect. The post-attack phase involves restoring the system to normal pre-test configurations. It includes removing files, cleaning registry entries, and removing shares and connections. Analyzing all the results and presenting them in a comprehensive report is also the part of this phase. These reports include objectives, observations, all activities undertaken, and the results of test activities, and may recommend fixes for vulnerabilities.

Question: 8

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

Answer: A, B, C

Explanation:
The main objectives of Business Impact Assessment (BIA) are as follows:
Criticality prioritization: the entire critical business unit processes must be identified and prioritized, and the impact of a disruptive event must be evaluated. The non-time-critical business processes will need a lower priority rating for recovery than time-critical business processes.
Down-time estimation: The Maximum Tolerable Downtime (MTD) is estimated with the help of BIA, which the business can tolerate and still remain a viable company. For this reason, the longest period of time a critical process can remain interrupted before the company can never recover. It is often found that this time period is much shorter than estimated during the BIA process. This means that the company can tolerate only a much briefer period of interruption than was previously thought.
Resource requirements identification: The identification of the required resources for the critical processes is also performed at this time, with the most time sensitive processes receiving the most resource allocation.
Answer option D is incorrect. This is the invalid answer because performing vulnerability assessment is a

step taken by BIA to achieve the above mentioned goals.

Question: 9

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

Explanation:
A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and triggers for initiating planned actions.
Answer option B is incorrect. Disaster recovery is the process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster.
Answer option A is incorrect. It deals with the plans and procedures that identify and prioritize the critical business functions that must be preserved.
Answer option C is incorrect. It includes the plans and procedures documented that ensure the continuity of critical operations during any period where normal operations are impossible.

Question: 10

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

Explanation:
Internet Protocol Security (IPSec) is used with Layer 2 Tunneling Protocol (L2TP). It is a standard-based protocol that provides the highest level of virtual private network (VPN) security. IPSec can encrypt virtually everything above the networking layer. It secures both data and password.

Question: 11

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: A, C, D

Explanation:
The subphases of the maintenance phase in the life cycle model are as follows:
Request control: This phase manages the users' requests for changes to the software product and gathers information that can be used for managing this activity.
Change control: This phase is the most important step in the maintenance phase. Various issues are addressed by the change control phase. Some of them are as follows:
1.Recreating and analyzing the problem
2.Developing the changes and corresponding tests
3.Performing quality control
Release control: It is associated with issuing the latest release of the software. Release control phase involves deciding which requests will be included in the new release, archiving of the release, configuration management, quality control, distribution, and acceptance testing.
Answer option B is incorrect. This is not a valid option.
Reference: CISM Review Manual 2010, Contents: "Information security process management"

Question: 12

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

Explanation:
Non-repudiation is a mechanism which proves that the sender really sent a message. It provides an evidence of the identity of the senderand message integrity. It also prevents a person from denying the submission or delivery of the message and the integrity of its contents.
Answer option C is incorrect. Authentication is a process of verifying the identity of a person or network host.
Answer option B is incorrect. Confidentiality ensures that no one can read a message except the intended receiver.
Answer option D is incorrect. Integrity assures the receiver that the received message has not been altered in any way from the original.
Reference: "http://en.wikipedia.org/wiki/Non-repudiation"

Question: 13

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.

Answer: A, B, C

Explanation:
The characteristics of the DIAP Information Readiness Assessment function are as follows:
It provides data needed to accurately assess IA readiness.
It identifies and generates IA requirements.
It performs vulnerability/threat analysis assessment.
Answer option D is incorrect. It is a function performed by the ASSET system.
Reference: CISM Review Manual 2010, Contents: "Information Security Program Development"