Free Questions for ISSMP by braindumpscollection

Shared by Slater on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **FillInTheBlank**

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.

Answer:

Explanation:

Additionally, OPSEC planners, working closely with Public Affairs personnel, must develop the Essential Elements of Friendly Information (EEFI) used to preclude inadvertent public disclosure of critical or sensitive information.

Question 2

Question Type: **MultipleChoice**

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?

Options:

A- Business continuity plan development

B- Business impact assessment

C- Scope and plan initiation

D- Plan approval and implementation

Answer:

A

Explanation:

The business continuity plan development refers to the utilization of the information collected in the Business Impact Analysis (BIA) for the creation of the recovery strategy plan to support the critical business functions. The information gathered from the BIA is mapped out to make a strategy for creating a continuity plan. The business continuity plan development process includes the areas of plan implementation, plan testing, and ongoing plan maintenance. This phase also consists of defining and documenting the continuity strategy.

Answer option C is incorrect. The scope and plan initiation process in BCP symbolizes the beginning of the BCP process. It emphasizes on creating the scope and the additional elements required to define the parameters of the plan.

The scope and plan initiation phase embodies a check of the company's operations and support services. The scope activities include creating a detailed account of the work required, listing the resources to be used, and defining the management practices to be employed.

Answer option B is incorrect. The business impact assessment is a method used to facilitate business units to understand the impact of a disruptive event. This phase includes the execution of a vulnerability assessment. This process makes out the mission-critical areas and business processes that are important for the survival of business.

It is similar to the risk assessment process. The function of a business impact assessment process is to create a document, which is used to help and understand what impact a disruptive event would have on the business.

Answer option D is incorrect. The plan approval and implementation process involves creating enterprise-wide awareness of the plan, getting the final senior management signoff, and implementing a maintenance procedure for updating the plan as required.

Question 3

Question Type: MultipleChoice

Which of the following statements is related with the second law of OPSEC?

Options:

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

Explanation:

OPSEC is also known as operations security. It has three laws.

The First Law of OPSEC. If you don't know the threat, how do you know what to protect? Although specific threats may vary from site to site or program to program. Employees must be aware of the actual and postulated threats. In any given situation, there is likely to be more than one adversary, although each may be interested in different information.

The Second Law of OPSEC. If you don't know what to protect, how do you know you are protecting it? The 'what' is the critical and sensitive, or target, information that adversaries require to meet their objectives.

The Third Law of OPSEC. If you are not protecting it (the critical and sensitive information), the adversary wins! OPSEC vulnerability assessments, (referred to as 'OPSEC assessments' - OA's - or sometimes as Surveys') are conducted to determine whether or not critical information is vulnerable to exploitation. An OA is a critical analysis of 'what we do' and 'how we do it' from the perspective of

an adversary. Internal procedures and information sources are also reviewed to determine whether there is an inadvertent release of sensitive information.

Answer option D is incorrect. The statement given in the option is not a valid law of OPSEC.

Question 4

Question Type: MultipleChoice

Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?

Options:

A- Safeguard

B- Single Loss Expectancy (SLE)

C- Exposure Factor (EF)

D- Annualized Rate of Occurrence (ARO)

Answer:

D

Explanation:

The Annualized Rate of Occurrence (ARO) is a number that represents the estimated frequency at which a threat is expected to occur. It is calculated based upon the probability of the event occurring and the number of employees that could make that event occur.

Answer option C is incorrect. The Exposure Factor (EF) represents the % of assets loss caused by a threat. The EF is required to calculate the Single Loss Expectancy (SLE).

Answer option A is incorrect. Safeguard acts as a countermeasure for reducing the risk associated with a specific threat or a group of threats.

Answer option B is incorrect. Single Loss Expectancy is a term related to Risk Management and Risk Assessment. It can be defined as the monetary value expected from the occurrence of a risk on an asset. It is mathematically expressed as follows.

Single Loss Expectancy (SLE) = Asset Value (AV) * Exposure Factor (EF)

where the Exposure Factor is represented in the impact of the risk over the asset, or percentage of asset lost. As an example, if the Asset Value is reduced two thirds, the exposure factor value is .66. If the asset is completely lost, the Exposure Factor is 1.0. The result is a monetary value in the same unit as the Single Loss Expectancy is expressed.

Question 5

Question Type: **MultipleChoice**

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

Options:

A- Evidence access policy

B- Incident response policy

C- Chain of custody

D- Chain of evidence

Answer:

C

Explanation:

A chain of custody is a documentation that shows who has collected and accessed each piece of evidence. The documentation must be meticulously prepared including the minutest details (such as the date, time, location, and the verified identity of every person handling the evidence) so that the documentation is verifiable. It includes the time of accessing the evidence and the valid reason for doing so. A chain of custody must be maintained for all evidences in order to maintain the validity of the evidences.

Answer option B is incorrect. Incident response policy is a document that defines an incident and helps people to respond appropriately to that incident. It provides information about people who are responsible for handling security incidents and how they can be contacted. The

incident response policy also provides instructions to deal with documenting and disseminating incident-related information.

Question 6

Question Type: MultipleChoice

Which of the following is generally practiced by the police or any other recognized governmental authority?

Options:

A- Phishing

B- Wiretapping

C- SMB signing

D- Spoofing

Answer:

B

Explanation:

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.

Answer option C is incorrect. Server Message Block (SMB) signing is a security feature of Windows operating systems. SMB signing ensures that the transmission and reception of files across a network are not altered in any way. As the traditional SMB authentication is vulnerable to man-in-the-middle (MITM) attacks, the secure transmission of SMB traffic is required. Implementing mutual authentication SMB signing protects a network from these attacks. The SMB signing feature adds digital signatures into SMB packets to strengthen SMB authentication.

Note. Enabling SMB signing on the network reduces the performance of the network because of the increased processing and network traffic required to digitally sign each SMB packet.

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 A is incorrect. Phishing is a type of scam that entice a user to disclose personal information such as social security number, bank account details, or credit card number. An example of phishing attack is a fraudulent e-mail that appears to come from a user's bank asking to change his online banking password. When the user clicks the link available on the e-mail, it directs him to a phishing site which replicates the original bank site. The phishing site lures the user to provide his personal information.