CSSLP^{Q&As}

Certified Secure Software Lifecycle Professional Practice Test

Pass ISC CSSLP Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/csslp.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by ISC Official Exam Center

QUESTION 1

You are the project manager for your organization. You are preparing for the quantitative risk analysis. Mark, a project team member, wants to know why you need to do quantitative risk analysis when you just completed qualitative risk analysis. Which one of the following statements best defines what quantitative risk analysis is?

A. Quantitative risk analysis is the process of prioritizing risks for further analysis or action by assessing and combining their probability of occurrence and impact.

B. Quantitative risk analysis is the review of the risk events with the high probability and the highest impact on the project objectives.

C. Quantitative risk analysis is the planning and quantification of risk responses based on probability and impact of each risk event.

D. Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives.

Correct Answer: D

Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives. It is performed on risk that have been prioritized through the qualitative risk analysis process. Answer: A is incorrect. This is actually the definition of qualitative risk analysis. Answer: B is incorrect. While somewhat true, this statement does not completely define the quantitative risk analysis process. Answer: C is incorrect. This is not a valid statement about the quantitative risk analysis process. Risk response planning is a separate project management process.

QUESTION 2

Billy is the project manager of the HAR Project and is in month six of the project. The project is scheduled to last for 18 months. Management asks Billy how often the project team is participating in risk reassessment in this project. What should Billy tell management if he\\'s following the best practices for risk management?

A. Project risk management happens at every milestone.

B. Project risk management has been concluded with the project planning.

C. Project risk management is scheduled for every month in the 18-month project.

D. At every status meeting the project team project risk management is an agenda item.

Correct Answer: D

Risk management is an ongoing project activity. It should be an agenda item at every project status meeting. Answer: A is incorrect. Milestones are good times to do reviews, but risk management should happen frequently. Answer: C is incorrect. This answer would only be correct if the project has a status meeting just once per month in the project. Answer: B is management happens throughout the project as does project planning.

QUESTION 3

Which of the following statements describe the main purposes of a Regulatory policy? Each correct answer represents a complete solution. Choose all that apply.

A. It acknowledges the importance of the computing resources to the business model

B. It provides a statement of support for information security throughout the enterprise

C. It ensures that an organization is following the standard procedures or base practices of operation in its specific industry.

D. It gives an organization the confidence that it is following the standard and accepted industry policy.

Correct Answer: CD

The main purposes of a Regulatory policy are as follows: It ensures that an organization is following the standard procedures or base practices of operation in its specific industry. It gives an organization the confidence that it is following the standard and accepted industry policy. Answer: B and A are incorrect. These are the policy elements of Senior Management Statement of Policy.

QUESTION 4

You work as a Network Auditor for Net Perfect Inc. The company has a Windows-based network. While auditing the company\\'s network, you are facing problems in searching the faults and other entities that belong to it. Which of the following risks may occur due to the existence of these problems?

A. Residual risk

B. Secondary risk

C. Detection risk

D. Inherent risk

Correct Answer: C

Detection risks are the risks that an auditor will not be able to find what they are looking to detect. Hence, it becomes tedious to report negative results when material conditions (faults) actually exist. Detection risk includes two types of risk: Sampling risk: This risk occurs when an auditor falsely accepts or erroneously rejects an audit sample. Nonsampling risk: This risk occurs when an auditor fails to detect a condition because of not applying the appropriate procedure or using procedures inconsistent with the audit objectives (detection faults). Answer: A is incorrect. Residual risk is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures). The formula to calculate residual risk is (inherent risk) x (control risk) where inherent risk is (threats vulnerability). In the economic context, residual means "the quantity left over at the end of a process; a remainder". Answer: D is incorrect. Inherent risk, in auditing, is the risk that the account or section being audited is materially misstated without considering internal controls due to error or fraud. The assessment of inherent risk depends on the professional judgment of the auditor, and it is done after assessing the business environment of the entity being audited. Answer: B is incorrect. A secondary risk is a risk that arises as a straight consequence of implementing a risk response. The secondary risk is an outcome of dealing with the original risk. Secondary risks are not as rigorous or important as primary risks, but can turn out to be so if not estimated and planned properly.

QUESTION 5

Samantha works as an Ethical Hacker for we-are-secure Inc. She wants to test the security of the we-are-secure server for DoS attacks. She sends large number of ICMP ECHO packets to the target computer. Which of the following DoS attacking techniques will she use to accomplish the task?

A. Smurf dos attack

B. Land attack

C. Ping flood attack

D. Teardrop attack

Correct Answer: C

According to the scenario, Samantha is using the ping flood attack. In a ping flood attack, an attacker sends a large number of ICMP packets to the target computer using the ping command, i.e., ping -f target_IP_address. When the target computer receives these packets in large quantities, it does not respond and hangs. However, for such an attack to take place, the attacker must have sufficient Internet bandwidth, because if the target responds with an "ECHO reply ICMP packet" message, the attacker must have both the incoming and outgoing bandwidths available for communication. Answer: A is incorrect. In a smurf DoS attack, an attacker sends a large amount of ICMP echo request traffic to the IP broadcast addresses. These ICMP requests have a spoofed source address of the intended victim. If the routing device delivering traffic to those broadcast addresses delivers the IP broadcast to all the hosts, most of the IP addresses send an ECHO reply message. However, on a multi- access broadcast network, hundreds of computers might reply to each packet when the target network is overwhelmed by all the messages sent simultaneously. Due to this, the network becomes unable to provide services to all the messages and crashes. Answer: D is incorrect. In a teardrop attack, a series of data packets are sent to the target computer with overlapping offset field values. As a result, the target computer is unable to reassemble these packets and is forced to crash, hang, or reboot. Answer: B is incorrect. In a land attack, the attacker sends a spoofed TCP SYN packet in which the IP address of the target is filled in both the source and destination fields. On receiving the spoofed packet, the target system becomes confused and goes into a frozen state. Now-a-days, antivirus can easily detect such an attack.