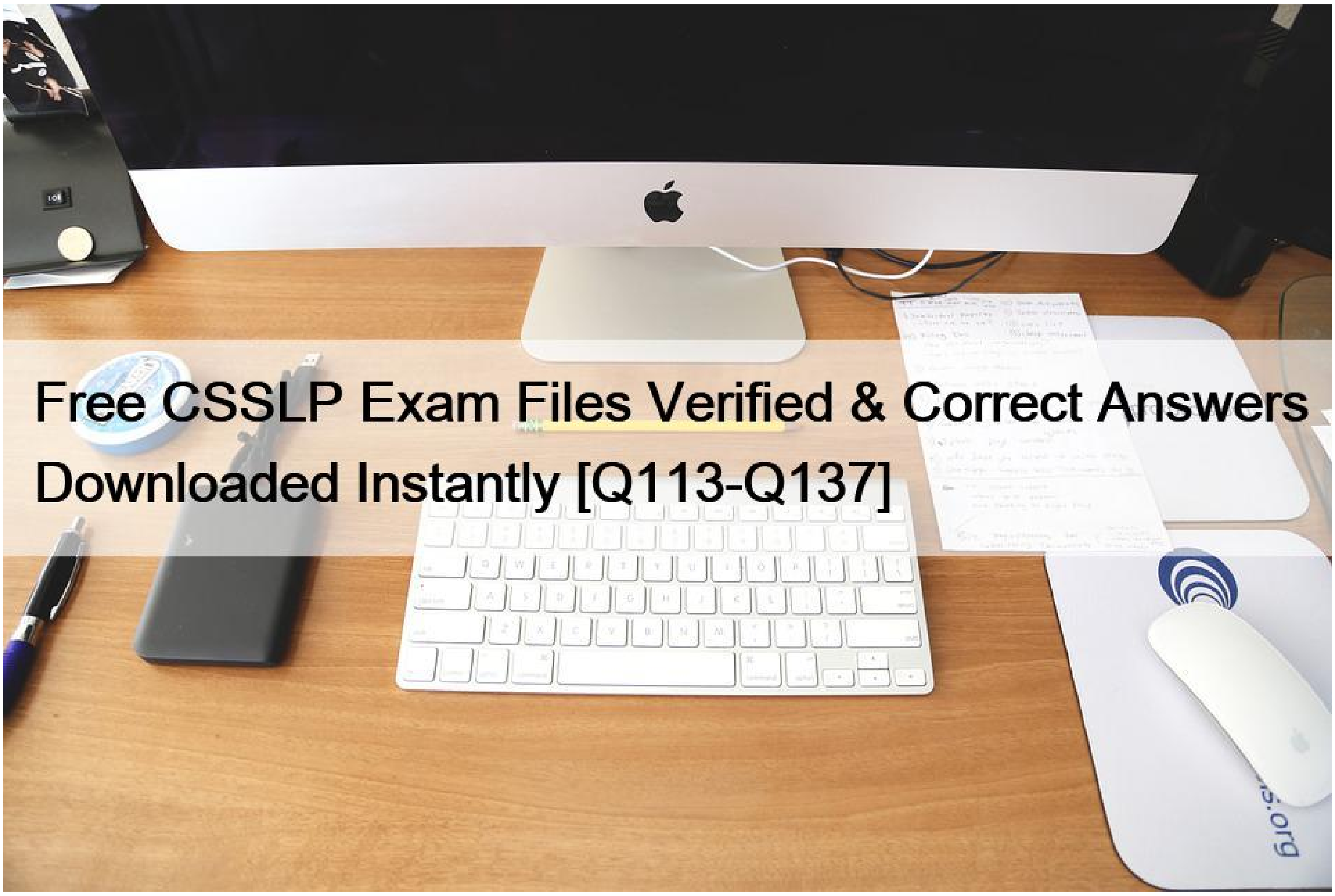
Free CSSLP Exam Files Verified & Correct Answers Downloaded Instantly [Q113-Q137


Free CSSLP Exam Files Verified & Correct Answers Downloaded Instantly [Q113-Q137]

Free CSSLP Exam Files Verified & Correct Answers Downloaded Instantly Instant Download CSSLP Dumps Q&As Provide PDF&Test Engine

Secure Software Testing (14%): - Track and classify security errors;- Establish security test cases;- Secure test data;- Validate documentations;- Develop a strategy and plan for security testing;

Career Opportunities

(ISC)2 CSSLP is an ideal option for the security professionals and software development specialists because it helps fortify and validate their skills to perform the required tasks efficiently. The individuals with this certificate can explore numerous career opportunities and take up the job titles as a Security Manager, a Cybersecurity Engineer, and a Security Consultant. They can also work as Information Managers, Information Security Consultants, Testing Managers, Information Security Managers, and IT Security Analysts. Their income will depend on their role, but looking at a possible average salary, they can expect about $98,000 per year.

QUESTION 113

Which of the following intrusion detection systems (IDS) monitors network traffic and compares it against an established baseline?

- File-based
- Network-based
- Anomaly-based
- Signature-based

Explanation/Reference:

Explanation: The anomaly-based intrusion detection system (IDS) monitors network traffic and compares it against an established baseline. This type of IDS monitors traffic and system activity for unusual behavior based on statistics. In order to identify a malicious activity, it learns normal behavior from the baseline. The anomaly-based intrusion detection is also known as behavior-based or statistical-based intrusion detection. AnswerD is incorrect. Signature-based IDS uses a database with signatures to identify possible attacks and malicious activity. Answer B is incorrect. A network-based IDS can be a dedicated hardware appliance, or an application running on a computer, attached to the network. It monitors all traffic in a network or traffic coming through an entry-point such as an Internet connection. Answer: A is incorrect.

There is no such intrusion detection system (IDS) that is file-based.

QUESTION 114

In which of the following types of tests are the disaster recovery checklists distributed to the members of disaster recovery team and asked to review the assigned checklist?

- Parallel test
- Simulation test
- Full-interruption test
- Checklist test

Explanation/Reference:

Explanation: A checklist test is a test in which the disaster recovery checklists are distributed to the members of the disaster recovery team. All members are asked to review the assigned checklist. The checklist test is a simple test and it is easy to conduct this test. It allows to accomplish the following three goals: It ensures that the employees are aware of their responsibilities and they have the refreshed knowledge. It provides an individual with an opportunity to review the checklists for obsolete information and update any items that require modification during the changes in the organization. It ensures that the assigned members of disaster recovery team are still working for the organization. Answer: B is incorrect.

A simulation test is a method used to test the disaster recovery plans. It operates just like a structured walk- through test. In the simulation test, the members of a disaster recovery team present with a disaster scenario and then, discuss on appropriate responses. These suggested responses are measured and some of them are taken by the team. The range of the simulation test should be defined carefully for avoiding excessive disruption of normal business activities. Answer: A is incorrect. A parallel test includes the next level in the testing procedure, and relocates the employees to an alternate recovery site and implements site activation procedures. These employees present with their disaster recovery responsibilities as they would for an actual disaster. The disaster recovery sites have full responsibilities to conduct the day-to-day organization&#8217;s business. Answer: C is incorrect. A full-interruption test includes the operations that shut down at the primary site and are shifted to the recovery site according to the disaster recovery plan. It operates just like a parallel test. The full-interruption test is very expensive and difficult to arrange. Sometimes, it causes a major disruption of operations if the test fails.

QUESTION 115

Which of the following tiers addresses risks from an information system perspective?

- Tier 0
- Tier 3

* Tier 2
* Tier 1
Explanation/Reference:

Explanation: The information system level is the tier 3. It addresses risks from an information system perspective, and is guided by the risk decisions at tiers 1 and 2. Risk decisions at tiers 1 and 2 impact the ultimate selection and deployment of requisite safeguards. This also has an impact on the countermeasures at the information system level. The RMF primarily operates at tier3 but it can also have interactions at tiers 1 and 2. AnswerA is incorrect. It is an invalid Tier description. Answer: D is incorrect.

The Organization Level is the Tier 1, and it addresses risks from an organizational perspective. AnswerC is incorrect. The mission and business process level is the Tier 2, and it addresses risks from the mission and business process perspective.

QUESTION 116

Which of the following scanning techniques helps to ensure that the standard software configuration is currently with the latest security patches and software, and helps to locate uncontrolled or unauthorized software?
* Port Scanning
* Discovery Scanning
* Server Scanning
* Workstation Scanning
Explanation/Reference:

Explanation: Workstation scanning provides help to ensure that the standard software configuration exists with the most recent security patches and software. It helps to locate uncontrolled or unauthorized software. A full workstation vulnerability scan of the standard corporate desktop configuration must be implemented on a regularly basis. AnswerB is incorrect. The discovery scanning technique is used to gather adequate information regarding each network device to identify what type of device it is, its operating system, and if it is running any externally vulnerable services, like Web services, FTP, or email.

AnswerC is incorrect. A full server vulnerability scan helps to determine if the server OS has been

configured to the corporate standards and identify if applications have been updated with the latest security patches and software versions. AnswerA is incorrect. Port scanning technique describes the process of sending a data packet to a port to gather information about the state of the port.

QUESTION 117

The organization level is the Tier 1 and it addresses risks from an organizational perspective. What are the various Tier 1 activities? Each correct answer represents a complete solution. Choose all that apply.
* The organization plans to use the degree and type of oversight, to ensure that the risk management strategy is being effectively carried out.
* The level of risk tolerance.
* The techniques and methodologies an organization plans to employ, to evaluate information system-related security risks.
* The RMF primarily operates at Tier 1.
The Organization Level is the Tier 1, and it addresses risks from an organizational perspective. It includes the following points: The techniques and methodologies an organization plans to employ, to evaluate information system-related security risks. During risk assessment, the methods and procedures the organization plans to use, to evaluate the significance of the risks identified. The types and extent of risk mitigation measures the organization plans to employ, to address identified risks. The level of risk tolerance. According to the environment of operation, how the organization plans to monitor risks on an ongoing basis, given the inevitable changes to organizational information system. The organization plans to use the degree and type of oversight, in order to ensure that the risk management strategy is being effectively carried out. Answer D is incorrect. The RMF primarily operates at Tier 3.

QUESTION 118

Which of the following processes culminates in an agreement between key players that a system in its current configuration and operation provides adequate protection controls?
* Information Assurance (IA)
* Information systems security engineering (ISSE)
* Certification and accreditation (C&A)
* Risk Management
Explanation/Reference:

Explanation: Certification and accreditation (C&A) is a set of processes that culminate in an agreement between key players that a system in its current configuration and operation provides adequate protection controls. Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The C&A process is used extensively in the U.S. Federal Government. Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed- upon set of security controls. Answer: D is incorrect. Risk management is a set of processes that ensures a risk-based approach is used to determine adequate, cost- effective security for a system. Answer: A is incorrect. Information assurance (IA) is the process of organizing and monitoring information-related risks.

It ensures that only the approved users have access to the approved information at the approved time. IA practitioners seek to protect and defend information and information systems by ensuring confidentiality, integrity, authentication, availability, and non-repudiation. These objectives are applicable whether the information is in storage, processing, or transit, and whether threatened by an attack. Answer: B is incorrect. ISSE is a set of processes and solutions used during all phases of a system&#8217;s life cycle to meet the system&#8217;s information protection needs.

QUESTION 119

Digital rights management (DRM) consists of compliance and robustness rules. Which of the following features does the robustness rule have? Each correct answer represents a complete solution. Choose three.
* It specifies the various levels of robustness that are needed for asset security.
* It specifies minimum techniques for asset security.
* It specifies the behaviors of the DRM implementation and applications accessing the implementation.
* It contains assets, such as device key, content key, algorithm, and profiling data.
Explanation/Reference:

Explanation: The DRM (digital rights management) technology includes the following rules: 1.Compliance rule: This rule specifies the behaviors of the DRM implementation, and applications that are accessing the implementation. The compliance rule specifies the following elements: Definition of specific license rights Device requirements Revocation of license path or penalties when the implementation is not robust enough or noncompliant 2.Robustness rule: This rule has the following features: It specifies the various levels of robustness that are needed for asset security. It contains assets, such as device key, content key, algorithm, and profiling data. It specifies minimum techniques for asset security.

QUESTION 120

An assistant from the HR Department calls you to ask the Service Hours & Maintenance Slots for your ERP system. In which document will you most probably find this information?

* Service Level Agreement
* Release Policy
* Service Level Requirements
* Underpinning Contract

You will most probably find this information in the Service Level Agreement document. Amongst other information, SLA contains information about the agreed Service Hours and maintenance slots for any particular Service. Service Level Agreement (frequently abbreviated as SLA) is a part of a service contract where the level of service is formally defined. In practice, the term SLA is sometimes used to refer to the contracted delivery time (of the service) or performance. Service Level Agreement (SLA) is a negotiated agreement between two parties where one is the customer and the other is the service provider. This can be a legally binding formal or informal &#8216;contract&#8217;. Contracts between the Service Provider and other third parties are often (incorrectly) called SLAs, as the level of service has been set by the (principal) customer there can be no &#8216;agreement&#8217; between third parties (these agreements are simply a &#8216;contract&#8217;). Operating Level Agreements or OLA(s) however, may be used by internal groups to support SLA (s). Answer B is incorrect. Release Policy is a set of rules for deploying releases into the live operational environment, defining different approaches for releases depending on their urgency and impact. Answer C is incorrect. The Service Level Requirements document contains the requirements for a service from the client viewpoint, defining detailed service level targets, mutual responsibilities, and other requirements specific to a certain group of customers. Answer D is incorrect. Underpinning Contract (UC) is a contract between an IT service provider and a third party. In another way, it is an agreement between the IT organization and an external provider about the delivery of one or more services. The third party provides services that support the delivery of a service to a customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level targets in an SLA.

QUESTION 121

You work as a Security Manager for Tech Perfect Inc. You have set up a SIEM server for the following purposes: Analyze the data from different log sources Correlate the events among the log entries Identify and prioritize significant events Initiate responses to events if required One of your log monitoring staff wants to know the features of SIEM product that will help them in these purposes. What features will you recommend? Each correct answer represents a complete solution. Choose all that apply.

* Asset information storage and correlation
* Transmission confidentiality protection
* Incident tracking and reporting
* Security knowledge base
* Graphical user interface

Explanation/Reference:

Explanation: The features of SIEM products are as follows: Graphical user interface (GUI): It is used in analysis for identifying potential problems and reviewing all available data that are associated with the problems. Security knowledge base: It includes information on known vulnerabilities, log messages, and other technical data. Incident tracking and hacking: It has robust workflow features to track and report incidents. Asset information storage and correlation: It gives higher priority to an attack that affects a vulnerable OS or a main host. Answer: B is incorrect. SIEM product does not have this feature.

QUESTION 122

There are seven risks responses that a project manager can choose from. Which risk response is appropriate for both positive and negative risk events?

* Acceptance
* Transference
* Sharing
* Mitigation

Only acceptance is appropriate for both positive and negative risk events. Often sharing is used for low probability and low impact risk events regardless of the positive or negative effects the risk event may bring the project. Acceptance response is a part of Risk Response planning process. Acceptance response delineates that the project plan will not be changed to deal with the risk. Management may develop a contingency plan if the risk does occur. Acceptance response to a risk event is a strategy that can be used for risks that pose either threats or opportunities. Acceptance response can be of two types: Passive acceptance: It is a strategy in which no plans are made to try or avoid or mitigate the risk. Active acceptance: Such responses include developing contingency reserves to deal with risks, in case they occur. Acceptance is the only response for both threats and opportunities. Answer C is incorrect. Sharing is a positive risk response that shares an opportunity for all parties involved in the risk event. Answer B is incorrect. Transference is a negative risk event that transfers the risk ownership to a third party, such as vendor, through a contractual relationship. Answer D is incorrect. Mitigation is a negative risk event that seeks to lower the probability and/or impact of a risk event.

QUESTION 123

In digital rights management, the level of robustness depends on the various types of tools and attacks to which they must be resistant or immune. Which of the following types of tools are expensive, require skill, and are not easily available?
* Hand tools
* Widely available tools
* Specialized tools
* Professional tools
The tools used in DRM to define the level of robustness are as follows: 1.Widely available tools: These tools are easy to use and are available to everyone. For example, screwdrivers and file editors. 2.Specialized tools: These tools require skill and are available at reasonable prices. For example, debuggers, decompilers, and memory scanners. 3.Professional tools: These tools are expensive, require skill, and are not easily available. For example, logic analyzers, circuit emulators, and chip disassembly systems.

QUESTION 124

Which of the following types of attacks is targeting a Web server with multiple compromised computers that are simultaneously sending hundreds of FIN packets with spoofed IP source IP addresses?
* DDoS attack
* Evasion attack
* Insertion attack
* Dictionary attack
A distributed denial of service (DDoS) attack targets a Web server with multiple compromised computers that are simultaneously sending hundreds of FIN packets with spoofed IP source IP addresses. DDoS attack occurs when multiple compromised systems flood the bandwidth or resources of a targeted system, usually one or more Web servers. These systems are compromised by attackers using a variety of methods. It is an attempt to make a computer resource unavailable to its intended users. This type of attack can cause the following to occur: Saturate network resources. Disrupt connections between two computers, thereby preventing communications between services. Disrupt services on a specific computer. Answer D is incorrect. Dictionary attack is a type of password guessing attack. This type of attack uses a dictionary of common words to find out the password of a user. It can also use common words in either upper or lower case to find a password. There are many programs available on the Internet to automate and execute dictionary attacks. Answer C is incorrect. In an insertion attack, an IDS accepts a packet and assumes that the host computer will also accept it. But in reality, when a host system rejects the packet, the IDS accepts the attacking string that will exploit vulnerabilities in the IDS. Such attacks can badly infect IDS signatures and IDS signature analysis. Answer B is incorrect. An evasion attack is one in which an IDS rejects a malicious packet but the host computer accepts it. Since an IDS has rejected it, it does not check the contents of the packet. Hence, using this technique, an attacker can exploit the host computer. In many cases, it is quite simple for an attacker to send such data packets that can easily perform evasion attacks on an IDSs.

QUESTION 125

The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise. What are the responsibilities of a Chief Information Officer?

Each correct answer represents a complete solution. Choose all that apply.
* Facilitating the sharing of security risk-related information among authorizing officials
* Preserving high-level communications and working group relationships in an organization
* Establishing effective continuous monitoring program for the organization
* Proposing the information technology needed by an enterprise to achieve its goals and then working within a budget to implement the plan
Explanation/Reference:

Explanation: A Chief Information Officer (CIO) plays the role of a leader. The responsibilities of a Chief Information Officer are as follows: Establishes effective continuous monitoring program for the organization. Facilitates continuous monitoring process for the organizations. Preserves high-level communications and working group relationships in an organization.

Confirms that information systems are covered by a permitted security plan and monitored throughout the System Development Life Cycle (SDLC). Manages and delegates decisions to employees in large enterprises. Proposes the information technology needed by an enterprise to achieve its goals and then works within a budget to implement the plan. AnswerA is incorrect. A Risk Executive facilitates the sharing of security risk-related information among authorizing officials.

QUESTION 126

Which of the following is an attack with IP fragments that cannot be reassembled?
* Password guessing attack
* Teardrop attack
* Dictionary attack
* Smurf attack
Explanation/Reference:

Explanation: Teardrop is an attack with IP fragments that cannot be reassembled. In this attack, corrupt packets are sent to the victim&#8217;s computer by using IP&#8217;s packet fragmentation algorithm. As a result of this attack, the victim&#8217;s computer might hang. AnswerD is incorrect. Smurf is an ICMP attack that involves spoofing and flooding. AnswerC is incorrect. Dictionary attack is a type of password guessing attack. This type of attack uses a dictionary of common words to find out the password of a user. It can also use common words in either upper or lower case to find a password. There are many programs available on the Internet to automate and execute dictionary attacks. AnswerA is incorrect. A password guessing attack occurs when an unauthorized user tries to log on repeatedly to a computer or network by guessing usernames and passwords. Many password guessing programs that attempt to break passwords are available on the Internet. Following are the types of password guessing attacks: Brute force attack Dictionary attack

QUESTION 127

FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls are tested and reviewed?
* Level 4
* Level 5
* Level 2
* Level 3
* Level 1
Explanation/Reference:

Explanation: The following are the five levels of FITSAF based on SEI&#8217;s Capability Maturity Model (CMM):

Level 1: The first level reflects that an asset has documented a security policy. Level 2: The second level shows that the asset has documented procedures and controls to implement the policy. Level 3: The third level indicates that these procedures and controls have been implemented. Level 4: The fourth level shows that the procedures and controls are tested and reviewed. Level 5: The fifth level is the final level and shows that the asset has procedures and controls fully integrated into a comprehensive program.

QUESTION 128

You work as a security engineer for BlueWell Inc. Which of the following documents will you use as a guide for the security certification and accreditation of Federal Information Systems?
* NIST Special Publication 800-60
* NIST Special Publication 800-53
* NIST Special Publication 800-37
* NIST Special Publication 800-59
NIST has developed a suite of documents for conducting Certification & Accreditation (C&A). These documents are as follows: NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems. NIST Special Publication 800-53: This document provides a guideline for security controls for Federal Information Systems. NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System. NIST Special Publication 800-59: This document is a guideline for identifying an information system as a National Security System. NIST Special Publication 800-60: This document is a guide for mapping types of information and information systems to security objectives and risk levels.

QUESTION 129

You are the project manager for a construction project. The project involves casting of a column in a very narrow space. Because of lack of space, casting it is highly dangerous. High technical skill will be required for casting that column. You decide to hire a local expert team for casting that column. Which of the following types of risk response are you following?
* Avoidance
* Acceptance
* Mitigation
* Transference
Explanation/Reference:

Explanation: According to the question, you are hiring a local expert team for casting the column. As you have transferred your risk to a third party, this is the transference risk response that you have adopted.

Transference is a strategy to mitigate negative risks or threats. In this strategy, consequences and the ownership of a risk is transferred to a third party. This strategy does not eliminate the risk but transfers responsibility of managing the risk to another party. Insurance is an example of transference. AnswerC is incorrect. Mitigation is a risk response planning technique associated with threats that seeks to reduce the probability of occurrence or impact of a risk to below an acceptable threshold. Risk mitigation involves taking early action to reduce the probability and impact of a risk occurring on the project. Adopting less complex processes, conducting more tests, or choosing a more stable supplier are examples of mitigation actions. Answer A is incorrect. Avoidance involves changing the project management plan to eliminate the threat entirely. Answer: B is incorrect. Acceptance response is a part of Risk Response planning process.

Acceptance response delineates that the project plan will not be changed to deal with the risk.

Management may develop a contingency plan if the risk does occur. Acceptance response to a risk event is a strategy that can be used for risks that pose either threats or opportunities. Acceptance response can be of two types: Passive acceptance: It is a strategy in which no plans are made to try or avoid or mitigate the risk. Active acceptance: Such responses include developing contingency reserves to deal with risks, in case they occur. Acceptance is the only response for both threats and opportunities.

QUESTION 130

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. In order to do so, he performs the following steps of the pre-attack phase successfully: Information gathering Determination of network range Identification of active systems Location of open ports and applications Now, which of the following tasks should he perform next?
* Perform OS fingerprinting on the We-are-secure network.
* Map the network of We-are-secure Inc.
* Install a backdoor to log in remotely on the We-are-secure server.
* Fingerprint the services running on the we-are-secure network.
Explanation/Reference:

Explanation: John will perform OS fingerprinting on the We-are-secure network. Fingerprinting is the easiest way to detect the Operating System (OS) of a remote system. OS detection is important because, after knowing the target system&#8217;s OS, it becomes easier to hack into the system. The comparison of data packets that are sent by the target system is done by fingerprinting. The analysis of data packets gives the attacker a hint as to which operating system is being used by the remote system. There are two types of fingerprinting techniques as follows: 1.Active fingerprinting 2.Passive fingerprinting In active fingerprinting ICMP messages are sent to the target system and the response message of the target system shows which OS is being used by the remote system. In passive fingerprinting the number of hops reveals the OS of the remote system. Answer: D and B are incorrect. John should perform OS fingerprinting first, after which it will be easy to identify which services are running on the network since there are many services that run only on a specific operating system. After performing OS fingerprinting, John should perform networking mapping. Answer: C is incorrect. This is a pre-attack phase, and only after gathering all relevant knowledge of a network should John install a backdoor.

QUESTION 131

In which of the following DIACAP phases is residual risk analyzed?
* Phase 1
* Phase 5
* Phase 2
* Phase 4
* Phase 3
The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk. The Certification Determination and Accreditation phase is the third phase in the DIACAP process. Its subordinate tasks are as follows: Analyze residual risk. Issue certification determination. Make accreditation decision. Answer A is incorrect. Phase 1 is known as Initiate and Plan IA C&A. Answer C is incorrect. Phase 2 is used to implement and validate assigned IA controls. Answer E is incorrect. Phase 3 is used to make certification determination and accreditation decisions. Answer B is incorrect. Phase 5 is known as decommission system and is used to conduct activities related to the disposition of the system data and objects.

QUESTION 132

The Project Risk Management knowledge area focuses on which of the following processes? Each correct answer represents a complete solution. Choose all that apply.
* Risk Monitoring and Control
* Risk Management Planning
* Quantitative Risk Analysis

* Potential Risk Monitoring
The Project Risk Management knowledge area focuses on the following processes: Risk Management Planning Risk Identification Qualitative Risk Analysis Quantitative Risk Analysis Risk Response Planning Risk Monitoring and Control Answer D is incorrect. There is no such process in the Project Risk Management knowledge area.

QUESTION 133

Bill is the project manager of the JKH Project. He and the project team have identified a risk event in the project with a high probability of occurrence and the risk event has a high cost impact on the project. Bill discusses the risk event with Virginia, the primary project customer, and she decides that the requirements surrounding the risk event should be removed from the project. The removal of the requirements does affect the project scope, but it can release the project from the high risk exposure. What risk response has been enacted in this project?
* Mitigation
* Transference
* Acceptance
* Avoidance
Explanation/Reference:

Explanation: This is an example of the avoidance risk response. Because the project plan has been changed to avoid the risk event, so it is considered the avoidance risk response. Risk avoidance is a technique used for threats. It creates changes to the project management plan that are meant to either eliminate the risk completely or to protect the project objectives from its impact. Risk avoidance removes the risk event entirely either by adding additional steps to avoid the event or reducing the project scope requirements. It may seem the answer to all possible risks, but avoiding risks also means losing out on the potential gains that accepting (retaining) the risk might have allowed. Answer: C is incorrect. Acceptance is when the stakeholders acknowledge the risk event and they accept that the event could happen and could have an impact on the project. Acceptance is usually used for risk events that have low risk exposure or risk events in which the project has no control, such as a pending law or weather threats. Answer: A is incorrect. Mitigation is involved with the actions to reduce an included risk&#8217;s probability and/or impact on the project&#8217;s objectives. As the risk was removed from the project, this scenario describes avoidance, not mitigation. Answer: B is incorrect. Transference is when the risk is still within the project, but the ownership and management of the risk event is transferred to a third party &#8211; usually for a fee.

QUESTION 134

You work as a Network Auditor for Net Perfect Inc. The company has a Windows-based network. While auditing the company&#8217;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?
* Residual risk
* Secondary risk
* Detection risk
* Inherent risk
Explanation/Reference:

Explanation: 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 &#8220;the quantity left over at the end of a process; a remainder&#8221;. 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 135

Which of the following are the important areas addressed by a software system&#8217;s security policy? Each correct answer represents a complete solution. Choose all that apply.
* Identification and authentication
* Punctuality
* Data protection
* Accountability
* Scalability
* Access control
The security policy of a software system addresses the following important areas: Access control Data protection Confidentiality Integrity Identification and authentication Communication security Accountability Answer E and B are incorrect. Scalability and punctuality are not addressed by a software system&#8217;s security policy.

QUESTION 136

John works as a systems engineer for BlueWell Inc. He has modified the software, and wants to retest the application to ensure that bugs have been fixed or not. Which of the following tests should John use to accomplish the task?
* Reliability test
* Functional test
* Performance test
* Regression test
Explanation/Reference:

Explanation: John should use the regression tests to retest the application to guarantee that bugs have been fixed. This test will help him to check that the earlier working functions have not failed as a result of the changes, and newly added features have not created problems with the previous versions. The various types of internal tests performed on builds are as follows: Regression tests: It is also known as the verification testing. These tests are developed to confirm that capabilities in earlier builds continue to work correctly in the subsequent builds. Functional test: These tests emphasizes on verifying that the build meets its functional and data requirements and correctly generates each expected display and report.

Performance tests: These tests are used to identify the performance thresholds of each build. Reliability tests: These tests are used to identify the reliability thresholds of each build.

QUESTION 137

You work as a systems engineer for BlueWell Inc. Which of the following tools will you use to look outside your own organization to examine how others achieve their performance levels, and what processes they use to reach those levels?
* Benchmarking
* Six Sigma
* ISO 9001:2000
* SEI-CMM

Explanation/Reference:

Explanation: Benchmarking is the tool used by system assessment process to provide a point of reference by which performance measurements can be reviewed with respect to other organizations. Benchmarking is also recognized as Best Practice Benchmarking or Process Benchmarking. It is a process used in management and mostly useful for strategic management. It is the process of comparing the business processes and performance metrics including cost, cycle time, productivity, or quality to another that is widely considered to be an industry standard benchmark or best practice. It allows organizations to develop plans on how to implement best practice with the aim of increasing some aspect of performance.

Benchmarking might be a one-time event, although it is frequently treated as a continual process in which organizations continually seek out to challenge their practices. It allows organizations to develop plans on how to make improvements or adapt specific best practices, usually with the aim of increasing some aspect of performance. Answer: C is incorrect. The ISO 9001:2000 standard combines the three standards

9001, 9002, and 9003 into one, called 9001. Design and development procedures are required only if a company does in fact engage in the creation of new products. The 2000 version sought to make a radical change in thinking by actually placing the concept of process management front and center (&#8220;Process management&#8221; was the monitoring and optimizing of a company&#8217;s tasks and activities, instead of just inspecting the final product). The ISO 9001:2000 version also demands involvement by upper executives, in order to integrate quality into the business system and avoid delegation of quality functions to junior administrators. Another goal is to improve effectiveness via process performance metrics numerical measurement of the effectiveness of tasks and activities. Expectations of continual process improvement and tracking customer satisfaction were made explicit. Answer: B is incorrect. Six Sigma is a business management strategy, initially implemented by Motorola. As of 2009 it enjoys widespread application in many sectors of industry, although its application is not without controversy. Six Sigma seeks to improve the quality of process outputs by identifying and removing the causes of defects and variability in manufacturing and business processes. It uses a set of quality management methods, including statistical methods, and creates a special infrastructure of people within the organization (&#8220;Black Belts&#8221;, &#8220;Green Belts&#8221;, etc.) who are experts in these methods. Each Six Sigma project carried out within an organization follows a defined sequence of steps and has quantified financial targets (cost reduction or profit increase).

The often used Six Sigma symbol is as follows:

Answer D is incorrect. Capability Maturity Model Integration (CMMI) was created by Software Engineering

Institute (SEI). CMMI in software engineering and organizational development is a process improvement approach that provides organizations with the essential elements for effective process improvement. It can be used to guide process improvement across a project, a division, or an entire organization. CMMI can help integrate traditionally separate organizational functions, set process improvement goals and priorities, provide guidance for quality processes, and provide a point of reference for appraising current processes.

CMMI is now the de facto standard for measuring the maturity of any process. Organizations can be assessed against the CMMI model using Standard CMMI Appraisal Method for Process Improvement (SCAMPI).

Exam Valid Dumps with Instant Download Free Updates: https://www.validbraindumps.com/CSSLP-exam-prep.html]