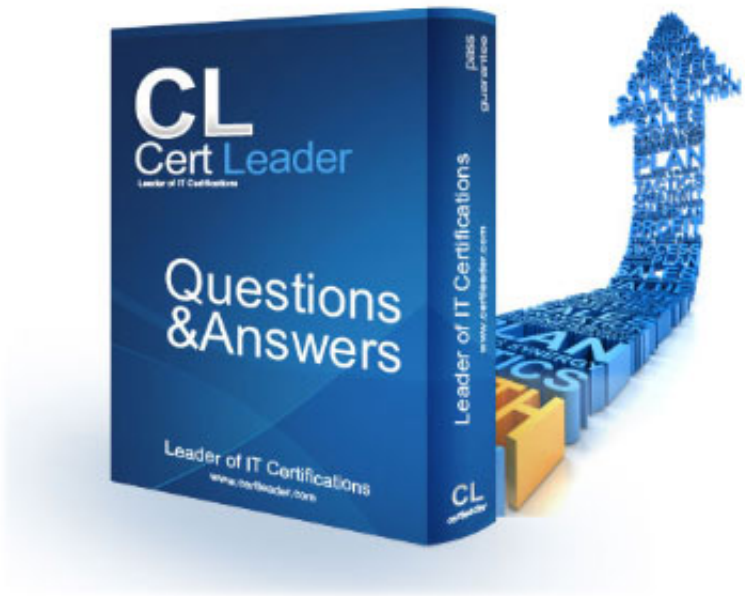
CSSLP - Certified Information Systems Security Professional

http://www.certleader.com/CSSLP-dumps.html



1. You and your project team have identified the project risks and now are analyzing the probability and impact of the risks. What type of analysis of the risks provides a quick and high-level review of each identified risk event?

A. Quantitative risk analysis

B. Qualitative risk analysis

C. Seven risk responses

D. A risk probability-impact matrix

Answer: B

Explanation: Qualitative risk analysis is a high-level, fast review of the risk event. Qualitative risk analysis qualifies the risk events for additional analysis.

2. Which of the following statements is true about residual risks?

A. It is the probabilistic risk after implementing all security measures.

B. It can be considered as an indicator of threats coupled with vulnerability.

C. It is a weakness or lack of safeguard that can be exploited by a threat.

D. It is the probabilistic risk before implementing all security measures.

Answer: A

Explanation: The residual risk is the risk or danger of an action or an event, a method or a (technical) process that still conceives these dangers even if all theoretically possible safety measures would be applied. The formula to calculate residual risk is (inherent risk) x (control risk) where inherent risk is (threats vulnerability). **Answer:** B is incorrect. In information security, security risks are considered as an indicator of threats coupled with vulnerability. In other words, security risk is a probabilistic function of a given threat agent exercising a particular vulnerability and the impact of that risk on the organization. Security risks can be mitigated by reviewing and taking responsible actions based on possible risks. **Answer:** C is incorrect. Vulnerability is a weakness or lack of safeguard that can be exploited by a threat, thus causing harm to the information systems or networks. It can exist in hardware , operating systems, firmware, applications, and configuration files. Vulnerability has been variously defined in the current context as follows: 1.A security weakness in a Target of Evaluation due to failures in analysis, design, implementation, or operation and such. 2.Weakness in an information system or components (e.g. system security procedures, hardware design, or internal controls that could be exploited to produce an information-related misfortune.) 3.The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the system, network, application, or protocol involved.

3. 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. User

E. Security auditor

Answer: B,C,D,E

Explanation: The following are the common roles with regard to data in an information classification program: Owner Custodian User Security auditor The following are the responsibilities of the owner with regard to data in an information classification program: Determining what level of classification the information requires. Reviewing the classification assignments at regular time intervals and making changes as the business needs change. Delegating the responsibility of the data protection duties to the custodian. The following are the responsibilities of the custodian with regard to data in an information classification program: Running regular backups and routinely testing the validity of the backup data Performing data restoration from the backups when necessary Controlling access, adding and removing privileges for individual users The users must comply with the requirements laid out in policies and procedures. They must also exercise due care. A security auditor examines an organization's security procedures and mechanisms.

4. Joseph works as a Software Developer for WebTech 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. Patent laws

C. Trademark laws

D. Copyright laws

Answer: B

Explanation: Patent laws are used to protect the duplication of software. Software patents cover the algorithms and techniques that are used in creating the software. It does not cover the entire program of the software. Patents give the author the right to make and sell his product. The time of the patent of a product is limited though, i.e., the author of the product has the right to use the patent for only a specific length of time. **Answer:** D is incorrect. Copyright laws protect original works or creations of authorship including literary, dramatic, musical, artistic, and certain other intellectual works.

5. 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.

A. The organization plans to use the degree and type of oversight, to ensure that the risk management strategy is being effectively carried out.

B. The level of risk tolerance.

C. The techniques and methodologies an organization plans to employ, to evaluate information system-related security risks.

D. The RMF primarily operates at Tier 1.

Answer: A,B,C

Explanation: 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.

6. Which of the following is a signature-based intrusion detection system (IDS) ?

A. RealSecure

B. StealthWatch

C. Tripwire

D. Snort

Answer: D

Explanation: Snort is a signature-based intrusion detection system. Snort is an open source network intrusion prevention and detection system that operates as a network sniffer. It logs activities of the network that is matched with the predefined signatures. Signatures can be designed for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP). The three main modes in which Snort can be configured are as follows: Sniffer mode: It reads the packets of the network and displays them in a continuous stream on the console. Packet logger mode: It logs the packets to the disk. Network intrusion detection mode: It is the most complex and configurable configuration, allowing Snort to analyze network traffic for matches against a user-defined rule set. **Answer:** B is incorrect. StealthWatch is a behavior-based intrusion detection system. **Answer:** A is incorrect. RealSecure is a network-based IDS that monitors TCP, UDP and ICMP traffic and is configured to look for attack patterns. **Answer:** C is incorrect. Tripwire is a file integrity checker for UNIX/Linux that can be used for host-based intrusion detection.

7. 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?

A. Parallel test

B. Simulation test

C. Full-interruption test

D. Checklist test

Answer: D

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'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.

8. To help review or design security controls, they can be classified by several criteria . One of these criteria is based on their nature. According to this criterion, which of the following controls consists of incident response processes, management oversight, security awareness, and training?

A. Compliance control

B. Physical control

C. Procedural control

D. Technical control

Answer: C

Explanation: Procedural controls include incident response processes, management oversight, security awareness, and training. **Answer:** B is incorrect. Physical controls include fences, doors, locks, and fire extinguishers. **Answer:** D is incorrect. Technical controls include user authentication (login) and logical access controls, antivirus software, and firewalls. **Answer:** A is incorrect. The legal and regulatory, or compliance controls, include privacy laws, policies, and clauses.

9. Which of the following is an example of over-the-air (OTA) provisioning in digital rights management?

A. Use of shared secrets to initiate or rebuild trust.

B. Use of software to meet the deployment goals.

C. Use of concealment to avoid tampering attacks.

D. Use of device properties for unique identification.

Answer: A

Explanation: Over- the- air provisioning is a mechanism to deploy MIDlet suites over a network. It is a method of distributing MIDlet suites. MIDlet suite providers install their MIDlet suites on Web servers and provide a hypertext link for downloading. A user can use this link to download the MIDlet suite either through the Internet microbrowser or through WAP on his device. Over-the-air provisioning is required for end-to-end encryption or other security purposes in order to deliver copyrighted software to a mobile device. For example, use of shared secrets to initiate or rebuild trust. **Answer:** D and C are incorrect. The use of device properties for unique identification and the use of concealment to avoid tampering attacks are the security challenges in digital rights management (DRM). **Answer:** B is incorrect. The use of software and hardware to meet the deployment goals is a distracter.

10. Which of the following access control models are used in the commercial sector? Each correct answer represents a complete solution. Choose two.

A. Biba model

B. Clark-Biba model

C. Clark-Wilson model

D. Bell-LaPadula model

Answer: A,C

Explanation: The Biba and Clark-Wilson access control models are used in the commercial sector. The Biba model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject. The Clark-Wilson security model provides a foundation for specifying and analyzing an integrity policy for a computing system. **Answer:** D is incorrect. The Bell-LaPadula access control model is mainly used in military systems. **Answer:** B is incorrect. There is no such access control model as Clark-Biba.

11. Which of the following types of redundancy prevents attacks in which an attacker can get physical control of a machine, insert unauthorized software, and alter data?

A. Data redundancy

B. Hardware redundancy

C. Process redundancy

D. Application redundancy

Answer: C

Explanation: Process redundancy permits software to run simultaneously on multiple geographically distributed locations, with voting on results. It prevents attacks in which an attacker can get physical control of a machine, insert unauthorized software, and alter data.

12. Which of the following cryptographic system services ensures that information will not be disclosed to any unauthorized person on a local network?

A. Authentication

B. Integrity

C. Non-repudiation

D. Confidentiality

Answer: D

Explanation: The confidentiality service of a cryptographic system ensures that information will not be disclosed to any unauthorized person on a local network.

13. You work as a project manager for BlueWell Inc. You are working on a project and the management wants a rapid and cost-effective means for establishing priorities for planning risk responses in your project. Which risk management process can satisfy management's objective for your project?

A. Qualitative risk analysis

B. Historical information

C. Rolling wave planning

D. Quantitative analysis

Answer: A

Explanation: Qualitative risk analysis is the best answer as it is a fast and low-cost approach to analyze the risk impact and its effect. It can promote certain risks onto risk response planning. Qualitative Risk Analysis uses the likelihood and impact of the identified risks in a fast and cost-effective manner. Qualitative Risk Analysis establishes a basis for a focused quantitative analysis or Risk Response Plan by evaluating the precedence of risks with a concern to impact on the project's scope, cost, schedule, and quality objectives. The qualitative risk analysis is conducted at any point in a project life cycle. The primary goal of qualitative risk analysis is to determine proportion of effect and theoretical response. The inputs to the Qualitative Risk Analysis process are: Organizational process assets Project Scope Statement Risk Management Plan Risk Register **Answer:** B is incorrect. Historical information can be helpful in the qualitative risk analysis, but it is not the best answer for the question as historical information is not always available (consider new projects). **Answer:** D is incorrect. Quantitative risk analysis is in-depth and often requires a schedule and budget for the analysis. **Answer:** C is incorrect. Rolling wave planning is not a valid answer for risk analysis processes.

14. Which of the following secure coding principles and practices defines the appearance of code listing so that a code reviewer and maintainer who have not written that code can easily understand it?

A. Make code forward and backward traceable

B. Review code during and after coding

C. Use a consistent coding style

D. Keep code simple and small

Answer: C

Explanation: Use a consistent coding style is one of the principles and practices that contribute to defensive coding. This principle defines the appearance of code listing so that a code reviewer and maintainer who have not written that code can easily understand it. For this purpose, all programmers of a team must follow the same guidelines. **Answer:** D is incorrect. Keep code simple and small defines that it is easy to verify the software security when a programmer uses small and simple code base. **Answer:** A is incorrect. Make code forward and backward traceable defines that traceability is necessary in order to validate requirements, prevent defects, and find and solve inconsistencies among all objects generated in the SDLC phases. **Answer:** B is incorrect. Review code during and after coding defines that code must be examined in order to identify coding errors in modules.

15. You are the project manager of the CUL project in your organization. You and the project team are assessing the risk events and creating a probability and impact matrix for the identified risks. Which one of the following statements best describes the requirements for the data type used in qualitative risk analysis?

A. A qualitative risk analysis encourages biased data to reveal risk tolerances.

B. A qualitative risk analysis required unbiased stakeholders with biased risk tolerances.

C. A qualitative risk analysis requires accurate and unbiased data if it is to be credible.

D. A qualitative risk analysis requires fast and simple data to complete the analysis.

Answer: C

Explanation: Of all the choices only this answer is accurate. The PMBOK clearly states that the data must be accurate and unbiased to be credible. **Answer:** D is incorrect. This is not a valid statement about the qualitative risk analysis dat**Answer:** A is incorrect. This is not a valid statement about the qualitative risk analysis dat**Answer:** B is incorrect. This is not a valid statement about the qualitative risk analysis data.

16. Which of the following methods determines the principle name of the current user and returns the jav a.security.Principal object in the HttpServletRequest interface?

A. getUserPrincipal()

B. isUserInRole()

C. getRemoteUser()

D. getCallerPrincipal()

Answer: A

Explanation: The getUserPrincipal() method determines the principle name of the current user and returns the java.security.Principal object. The java.security.Principal object contains the remote user name. The value of the getUserPrincipal() method returns null if no user is authenticated. **Answer:** C is incorrect. The getRemoteUser() method returns the user name that is used for the client authentication. The value of the getRemoteUser() method returns null if no user is authenticated. **Answer:** B is incorrect. The isUserInRole() method determines whether the remote user is granted a specified user role. The value of the isUserInRole() method returns true if the remote user is granted the specified user role;

otherwise it returns false. **Answer:** D is incorrect. The getCallerPrincipal() method is used to identify a caller using a java.security.Principal object. It is not used in the HttpServletRequest interface.

17. What are the various activities performed in the planning phase of the Software Assurance Acquisition process? Each correct answer represents a complete solution. Choose all that apply.

A. Develop software requirements.

B. Implement change control procedures.

C. Develop evaluation criteria and evaluation plan.

D. Create acquisition strategy.

Answer: A,C,D

Explanation: The various activities performed in the planning phase of the Software Assurance Acquisition process are as follows: Determine software product or service requirements. Identify associated risks. Develop software requirements. Create acquisition strategy. Develop evaluation criteria and evaluation plan. Define development and use of SwA due diligence questionnaires. **Answer:** B is incorrect. This activity is performed in the monitoring and acceptance phase of the Software Assurance acquisition process.

18. Which of the following organizations assists the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies?

A. OMB

B. NIST

C. NSA/CSS

D. DCAA

Answer: A

Explanation: The Office of Management and Budget (OMB) is a Cabinet-level office, and is the largest office within the Executive Office of the President (EOP) of the United States. The current OMB Director is Peter Orszag and was appointed by President Barack Obama. The OMB's predominant mission is to assist the

President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies. In helping to formulate the President's spending plans, the OMB evaluates the effectiveness of agency programs, policies, and procedures, assesses competing funding demands among agencies, and sets funding priorities. The OMB ensures that agency reports, rules, testimony, and proposed legislation are consistent with the President's Budget and with Administration policies.

Answer: D is incorrect. The DCAA has the aim to monitor contractor costs and perform contractor audits. **Answer:** C is incorrect. The National Security Agency/Central Security Service (NSA/CSS) is a crypto-logic intelligence agency of the United States government. It is administered as part of the United States Department of Defense. NSA is responsible for the collection and analysis of foreign communications and foreign signals intelligence, which involves cryptanalysis. NSA is also responsible for protecting U.S. government communications and information systems from similar agencies elsewhere, which involves cryptography. NSA is a key component of the U.S. Intelligence Community, which is headed by the Director of National Intelligence. The Central Security Service is a co- located agency created to coordinate intelligence activities and co-operation between NSA and U.S. military cryptanalysis agencies. NSA's work is limited to communications intelligence. It does not perform field or human intelligence activities. **Answer:** B is incorrect. The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.

19. 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?

A. Perform OS fingerprinting on the We-are-secure network.

B. Map the network of We-are-secure Inc.

C. Install a backdoor to log in remotely on the We-are-secure server.

D. Fingerprint the services running on the we-are-secure network.

Answer: A

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'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.

20. Which of the following roles is also known as the accreditor?

A. Data owner

B. Chief Risk Officer

C. Chief Information Officer

D. Designated Approving Authority

Answer: D

Explanation: Designated Approving Authority (DAA) is also known as the accreditor. **Answer:** A is incorrect. The data owner (information owner) is usually a member of management, in charge of a specific business unit, and is ultimately responsible for the protection and use of a specific subset of information. **Answer:** B is incorrect. A Chief Risk Officer (CRO) is also known as Chief Risk Management Officer (CRMO). The Chief Risk Officer or Chief Risk Management Officer of a corporation is the executive accountable for

enabling the efficient and effective governance of significant risks, and related opportunities, to a business and its various segments. Risks are commonly categorized as strategic, reputational, operational, financial, or compliance-related. CRO's are accountable to the Executive Committee and The Board for enabling the business to balance risk and reward. In more complex organizations, they are generally responsible for coordinating the organization's Enterprise Risk Management (ERM) approach. **Answer:** C is incorrect. The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise responsible for the information technology and computer systems that support enterprise goals. The CIO plays the role of a leader and reports to the chief executive officer, chief operations officer, or chief financial officer. In military organizations, they report to the commanding officer.

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CSSLP Exam with Our Prep Materials Via below:

http://www.certleader.com/CSSLP-dumps.html