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.leads4pass.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

Which of the following programming languages are compiled into machine code and directly executed by the CPU of a computer system? Each correct answer represents a complete solution. Choose two.

A. C

B. Microosft.NET

C. Java EE

D. C++

Correct Answer: AD

C and C++ programming languages are unmanaged code. Unmanaged code is compiled into machine code and directly executed by the CPU of a computer system. Answer: C and B are incorrect. Java EE and Microsoft.Net are compiled into an intermediate code format.

QUESTION 2

To help review or design security controls, they can be classified by several criteria. One of these criteria is based on time. According to this criteria, which of the following controls are intended to prevent an incident from occurring?

A. Corrective controls

B. Adaptive controls

C. Detective controls

D. Preventive controls

Correct Answer: D

Preventive controls are the security controls that are intended to prevent an incident from occurring, e.g., by locking out unauthorized intruders. Answer: C is incorrect. Detective controls are intended to identify and characterize an incident in progress, e.g., by sounding the intruder alarm and alerting the security guards or police. Answer: A is incorrect. Corrective controls are intended to limit the extent of any damage caused by the incident, e.g., by recovering the organization to normal working status as efficiently as possible. Answer: B is incorrect. There is no such categorization of controls based on time.

QUESTION 3

Which of the following strategies is used to minimize the effects of a disruptive event on a company, and is created to prevent interruptions to normal business activity?

A. Continuity of Operations Plan

B. Contingency Plan

C. Disaster Recovery Plan

D. Business Continuity Plan

Correct Answer: D

BCP is a strategy to minimize the consequence of the instability and to allow for the continuation of business processes. The goal of BCP is to minimize the effects of a disruptive event on a company, and is formed to avoid interruptions to normal business activity. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan. Answer: B is incorrect. A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. 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. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption. Answer: C is incorrect. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication, and reputation protection, and should refer to the disaster recovery plan (DRP) for IT-related infrastructure recovery/continuity. Answer: A is incorrect. The Continuity Of Operation Plan (COOP) refers to the preparations and institutions maintained by the United States government, providing survival of federal government operations in the case of catastrophic events. It provides procedures and capabilities to sustain an organization\\'s essential. COOP is the procedure documented to ensure persistent critical operations throughout any period where normal operations are unattainable.

QUESTION 4

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.

Correct Answer: ACD

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

QUESTION 5

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

Correct Answer: D

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

QUESTION 6

At which of the following levels of robustness in DRM must the security functions be immune to widely available tools and specialized tools and resistant to professional tools?

A. Level 2

B. Level 4

C. Level 1

D. Level 3

Correct Answer: C

At Level 1 of robustness in DRM, the security functions must be immune to widely available tools and specialized tools and resistant to professional tools.

QUESTION 7

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

Correct Answer: A

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.

QUESTION 8

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.

Correct Answer: A

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.

QUESTION 9

Microsoft software security expert Michael Howard defines some heuristics for determining code review in "A Process for Performing Security Code Reviews". Which of the following heuristics increase the application\\'s attack surface? Each correct answer represents a complete solution. Choose all that apply.

A. Code written in C/C++/assembly language

B. Code listening on a globally accessible network interface

C. Code that changes frequently

D. Anonymously accessible code

E. Code that runs by default

F. Code that runs in elevated context

Correct Answer: BDEF

Microsoft software security expert Michael Howard defines the following heuristics for determining code review in "A Process for Performing Security Code Reviews": Old code: Newer code provides better understanding of software security and has lesser number of vulnerabilities. Older code must be checked deeply. Code that runs by default: It must have high quality, and must be checked deeply than code that does not execute by default. Code that runs by default increases the application\\'s attack surface. Code that runs in elevated context: It must have higher quality. Code that runs in elevated privileges must be checked deeply and increases the application\\'s attack surface. Anonymously accessible code: It must be checked deeply than code that only authorized users and administrators can access, and it increases the application\\'s attack surface. Code listening on a globally accessible network interface: It must be checked deeply for security vulnerabilities and increases the application\\'s attack surface. Code written in C/C++/assembly language: It is prone to security vulnerabilities, for example, buffer overruns. Code with a history of security vulnerabilities: It includes additional vulnerabilities except concerted efforts that are required for removing them. Code that handles sensitive data: It must be checked deeply to ensure that data is protected from unintentional disclosure. Complex code: It includes undiscovered errors because it is more difficult to analyze complex code manually and programmatically. Code that changes frequently: It has more security vulnerabilities than code that does not change frequently.

QUESTION 10

Which of the following are the goals of risk management? Each correct answer represents a complete solution. Choose three.

A. Identifying the risk

B. Assessing the impact of potential threats

C. Identifying the accused

D. Finding an economic balance between the impact of the risk and the cost of the countermeasure

Correct Answer: ABD

There are three goals of risk management as follows: Identifying the risk Assessing the impact of potential threats Finding an economic balance between the impact of the risk and the cost of the countermeasure Answer: C is incorrect. Identifying the accused does not come under the scope of risk management.

QUESTION 11

Which of the following provides an easy way to programmers for writing lower-risk applications and retrofitting security into an existing application?

A. Watermarking

B. ESAPI

C. Encryption wrapper

D. Code obfuscation

Correct Answer: B

ESAPI (Enterprise Security API) is a group of classes that encapsulate the key security operations, needed by most of the applications. It is a free, open source, Web application security control library. ESAPI provides an easy way to programmers for writing lower-risk applications and retrofitting security into an existing application. It offers a solid foundation for new development. Answer: A is incorrect. Watermarking is the process of embedding information into software in a way that is difficult to remove. Answer: C is incorrect. Encryption wrapper dynamically encrypts and decrypts all the software code at runtime. Answer: D is incorrect. Code obfuscation is designed to protect code from decompilation.

QUESTION 12

DoD 8500.2 establishes IA controls for information systems according to the Mission Assurance Categories (MAC) and confidentiality levels. Which of the following MAC levels requires high integrity and medium availability?

A. MAC III

B. MAC IV

C. MAC I

D. MAC II

Correct Answer: D

The various MAC levels are as follows: MAC I: It states that the systems have high availability and high integrity. MAC II: It states that the systems have high integrity and medium availability. MAC III: It states that the systems have basic integrity and availability.

QUESTION 13

Adam works as a Computer Hacking Forensic Investigator for a garment company in the United States. A project has been assigned to him to investigate a case of a disloyal employee who is suspected of stealing design of the garments, which belongs to the company and selling those garments of the same design under different brand name. Adam investigated that the company does not have any policy related to the copy of design of the garments. He also investigated that the trademark under which the employee is selling the garments is almost identical to the original trademark of the company. On the grounds of which of the following laws can the employee be prosecuted?

A. Espionage law

B. Trademark law

C. Cyber law

D. Copyright law

Correct Answer: B

The Trademark law is a piece of legislation that contains the federal statutes of trademark law in the United States. The Act prohibits a number of activities, including trademark infringement, trademark dilution, and false advertising. Trademarks were traditionally protected in the United States only under State common law, growing out of the tort of unfair competition. Trademark law in the United States is almost entirely enforced through private lawsuits. The exception is in the case of criminal counterfeiting of goods. Otherwise, the responsibility is entirely on the mark owner to file suit in either state or federal civil court in order to restrict an infringing use. Failure to "police" a mark by stopping infringing uses can result in the loss of protection. Answer: D is incorrect. Copyright law of the United States governs the legally enforceable rights of creative and artistic works under the laws of the United States. Copyright law in the United States is part of federal law, and is authorized by the U.S. Constitution. The power to enact copyright law is granted in Article I, Section 8, Clause 8, also known as the Copyright Clause. This clause forms the basis for U.S. copyright law

("Science", "Authors", "Writings") and patent law ("useful Arts", "Inventors", "Discoveries"), and includes the limited terms (or durations) allowed for copyrights and patents ("limited Times"), as well as the items they may protect. In the U.S., registrations of claims of copyright, recordation of copyright transfers, and other administrative aspects of copyright are the responsibility of the United States Copyright Office, a part of the Library of Congress. Answer: A is incorrect. The Espionage Act of 1917 was a United States federal law passed shortly after entering World War I, on June 15, 1917, which made it a crime for a person: To convey information with intent to interfere with the operation or success of the armed forces of the United States or to promote the success of its enemies. This was punishable by death or by imprisonment for not more than 30 years. To convey false reports or false statements with intent to interfere with the operation or success of the military or naval forces of the United States or to promote the success of its enemies and whoever when the United States is at war, to cause or attempt to cause insubordination, disloyalty, mutiny, refusal of duty, in the military or naval forces of the United States, or to willfully obstruct the recruiting or enlistment service of the United States. Answer: C is incorrect. Cyber law is a very wide term, which wraps up the legal issue related to the use of communicative, transactional and distributive aspect of networked information device and technologies. It is commonly known as INTERNET LAW. These Laws are important to apply as Internet does not tend to make any geographical and jurisdictional boundaries clear; this is the reason why Cyber law is not very efficient. A single transaction may involve the laws of at least three jurisdictions, which are as follows: 1.The laws of the state/nation in which the user resides 2.The laws of the state/nation that apply where the server hosting the transaction is located 3.The laws of the state/nation, which apply to the person or business with whom the transaction takes place

QUESTION 14

Which of the following areas of information system, as separated by Information Assurance Framework, is a collection of local computing devices, regardless of physical location, that are interconnected via local area networks (LANs) and governed by a single security policy?

A. Local Computing Environments

B. Networks and Infrastructures

C. Supporting Infrastructures

D. Enclave Boundaries

Correct Answer: D

The areas of information system, as separated by Information Assurance Framework, are as follows: Local Computing Environments: This area includes servers, client workstations, operating system, and applications. Enclave Boundaries: This area consists of collection of local computing devices, regardless of physical location, that are interconnected via local area networks (LANs) and governed by a single security policy. Networks and Infrastructures: This area provides the network connectivity between enclaves. It includes operational area networks (OANs), metropolitan area networks (MANs), and campus area networks (CANs). Supporting Infrastructures: This area provides security services for networks, client workstations, Web servers, operating systems, applications, files, and single-use infrastructure machines

QUESTION 15

Which of the following is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention?

A. Copyright

B. Snooping

C. Utility model

D. Patent

Correct Answer: D

A patent is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention. Answer: A is incorrect. A copyright is a form of intellectual property, which secures to its holder the exclusive right to produce copies of his or her works of original expression, such as a literary work, movie, musical work or sound recording, painting, photograph, computer program, or industrial design, for a defined, yet extendable, period of time. It does not cover ideas or facts. Copyright laws protect intellectual property from misuse by other individuals. Answer: B is incorrect. Snooping is an activity of observing the content that appears on a computer monitor or watching what a user is typing. Snooping also occurs by using software programs to remotely monitor activity on a computer or network device. Hackers or attackers use snooping techniques and equipment such as keyloggers to monitor keystrokes, capture passwords and login information, and to intercept email and other private communications. Sometimes, organizations also snoop their employees legitimately to monitor their use of organizations\\' computers and track Internet usage. Answer: C is incorrect. A utility model is an intellectual property right to protect inventions.