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.pass2lead.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

In which of the following testing methodologies do assessors use all available documentation and work under no constraints, and attempt to circumvent the security features of an information system?

A. Full operational test

B. Penetration test

C. Paper test

D. Walk-through test

Correct Answer: B

A penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered. It is a component of a full security audit. Answer: C is incorrect. A paper test is the least complex test in the disaster recovery and business continuity testing approaches. In this test, the BCP/DRP plan documents are distributed to the appropriate managers and BCP/DRP team members for review, markup, and comment. This approach helps the auditor to ensure that the plan is complete and that all team members are familiar with their responsibilities within the plan. Answer: D is incorrect. A walk-through test is an extension of the paper testing in the business continuity and disaster recovery process. In this testing methodology, appropriate managers and BCP/DRP team members discuss and walk through procedures of the plan. They also discuss the training needs, and clarification of critical plan elements. Answer: A is incorrect. A full operational test includes all team members and participants in the disaster recovery and business continuity process. This full operation test involves the mobilization of personnel. It restores operations in the same manner as an outage or disaster would. The full operational test extends the preparedness test by including actual notification, mobilization of resources, processing of data, and utilization of backup media for restoration.

QUESTION 2

In which of the following processes are experienced personnel and software tools used to investigate, resolve, and handle process deviation, malformed data, infrastructure, or connectivity issues?

A. Risk Management

B. Exception management

C. Configuration Management

D. Change Management

Correct Answer: B

Exception management is a process in which experienced personnel and software tools are used to investigate, resolve, and handle process deviation, malformed data, infrastructure or connectivity issues. It increases the efficiency of business processes and contributes in the progress of business. Answer: C is incorrect. Configuration Management

(CM) is an Information Technology Infrastructure Library (ITIL) IT Service Management (ITSM) process. It tracks all of the individual Configuration Items (CI) in an IT system, which may be as simple as a single server, or as complex as the entire IT department. In large organizations a configuration manager may be appointed to oversee and manage the CM process. Answer: A is incorrect. Risk Management is used to identify, assess, and control risks. It includes analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats. Risk Management is part of Service Design and the owner of the Risk Management is the Risk Manager. Risks are addressed within several processes in ITIL V3; however, there is no dedicated Risk Management process. ITIL V3 calls for "coordinated risk assessment exercises", so at IT Process Maps we decided to assign clear responsibilities for managing risks. Answer: D is incorrect. Change Management is used to ensure that standardized methods and procedures are used for efficient handling of all changes. A change is "an event that results in a new status of one or more configuration items (CI\\'s)" approved by management, cost effective, enhances business process changes (fixes) - with a minimum risk to IT infrastructure. The main aims of Change Management are as follows: Minimal disruption of services Reduction in back-out Economic utilization of resources involved in the change

QUESTION 3

You work as a security manager for BlueWell Inc. You are going through the NIST SP 800-37 CandA methodology, which is based on four well defined phases. In which of the following phases of NIST SP 800-37 CandA methodology does the security categorization occur?

A. Security Accreditation

B. Security Certification

C. Continuous Monitoring

D. Initiation

Correct Answer: D

The various phases of NIST SP 800-37 CandA are as follows: Phase 1: Initiation- This phase includes preparation, notification and resource identification. It performs the security plan analysis, update, and acceptance. Phase 2: Security Certification- The Security certification phase evaluates the controls and documentation. Phase 3: Security Accreditation- The security accreditation phase examines the residual risk for acceptability, and prepares the final security accreditation package. Phase 4: Continuous Monitoring-This phase monitors the configuration management and control, ongoing security control verification, and status reporting and documentation.

QUESTION 4

Audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function. Under which of the following controls does audit control come?

A. Reactive controls

B. Detective controls

C. Protective controls

D. Preventive controls

Correct Answer: B

Audit trail or audit log comes under detective controls. Detective controls are the audit controls that are not needed to be restricted. Any control that performs a monitoring activity can likely be defined as a Detective Control. For example, it is possible that mistakes, either intentional or unintentional, can be made. Therefore, an additional Protective control is that these companies must have their financial results audited by an independent Certified Public Accountant. The role of this accountant is to act as an auditor. In fact, any auditor acts as a Detective control. If the organization in question has not properly followed the rules, a diligent auditor should be able to detect the deficiency which indicates that some control somewhere has failed. Answer: A is incorrect. Reactive or corrective controls typically work in response to a detective control, responding in such a way as to alert or otherwise correct an unacceptable condition. Using the example of account rules, either the internal Audit Committee or the SEC itself, based on the report generated by the external auditor, will take some corrective action. In this way, they are acting as a Corrective or Reactive control. Answer: C and D are incorrect. Protective or preventative controls serve to proactively define and possibly enforce acceptable behaviors. As an example, a set of common accounting rules are defined and must be followed by any publicly traded company. Each quarter, any particular company must publicly state its current financial standing and accounting as reflected by an application of these rules. These accounting rules and the SEC requirements serve as protective or preventative controls.

QUESTION 5

Which of the following security models dictates that subjects can only access objects through applications?

A. Biba model

B. Bell-LaPadula

C. Clark-Wilson

D. Biba-Clark model

Correct Answer: C

The Clark-Wilson security model dictates that subjects can only access objects through applications. Answer: A is incorrect. The Biba model does not let subjects write to objects at a higher integrity level. Answer: B is incorrect. The Bell-LaPadula model has a simple security rule, which means a subject cannot read data from a higher level. Answer: D is incorrect. There is no such model as Biba-Clark model.