CA1-001Q&As

CompTIA Advanced Security Practitioner (CASP) Beta Exam

Pass CompTIA CA1-001 Exam with 100% Guarantee

QUESTION 1

Which of the following processes is used to ensure that standardized methods and procedures are used for efficient handling of all changes?

A. Exception management

B. Configuration Management

C. Risk Management

D. Change Management

Correct Answer: D

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 (CIs)" 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 activities

Economic utilization of resources involved in the change Answer option B 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 option A is incorrect. 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 option C 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.

QUESTION 2

Which of the following are the benefits of the Single sign-on? Each correct answer represents a complete solution. Choose three.

A. Reducing password fatigue from different user name and password combinations

B. Increasing IT costs due to lower number of IT help desk calls about passwords

C. Centralized reporting for compliance adherence

D. Security on all levels of entry/exit/access to systems without the inconvenience of re-prompting users

Correct Answer: ACD

Following are the benefits of the Single sign-on:

Reduces phishing success, because users are not trained to enter password everywhere without thinking.

Reducing password fatigue from different user name and password combinations.

Reducing time spent re-entering passwords for the same identity.

Can support conventional authentications, such as windows credentials (i.e., username/password).

Reducing IT costs due to lower number of IT help desk calls about passwords.

Security on all levels of entry/exit/access to systems without the inconvenience of re-prompting users.

Centralized reporting for compliance adherence.

QUESTION 3

Risk assessment helps in determining the extent of potential threats and risks associated with an IT system throughout its SDLC. Which of the following steps covered by the risk assessment methodology?

Each correct answer represents a complete solution. Choose three.

A. Vulnerability Identification

B. Cost Analysis

C. Threat Identification

D. System Characterization

Correct Answer: ACD

Risk assessment is the first process of risk management. It helps in determining the extent of potential threats and risks associated with an IT system throughout its SDLC.

The risk assessment methodology covers nine steps which are as follows:

Step 1 - System Characterization

Step 2 - Threat Identification

Step 3 - Vulnerability Identification

Step 4 - Control Analysis

Step 5 - Likelihood Determination

Step 6 - Impact Analysis

Step 7 - Risk Determination

Step 8 - Control Recommendations

Step 9 - Results Documentation

QUESTION 4

John is concerned about internal security threats on the network he administers. He believes that he has taken every reasonable precaution against external threats, but is concerned that he may have gaps in his internal security. Which of the following is the most likely internal threat?

A. Employees not following security policy

B. Privilege Escalation

C. SQL Injection

D. Employees selling sensitive data

Correct Answer: A

Employees may disregard policies, such as policies limiting the use of USB devices or the ability to download programs from the internet. This is the most pervasive internal security threat. Answer option D is incorrect. Employees selling sensitive data is, of course, possible. However, this scenario is less likely that option A.

Answer option C is incorrect. SQL Injection is most likely accomplished by an external hacker. Answer option B is incorrect. Privilege escalation can be done by internal or external attackers. However, even with internal attackers, it is far less likely than option B.

QUESTION 5

Continuous Monitoring is the fourth phase of the Security Certification and Accreditation process, which of the following activities can be involved in the Continuous Monitoring process?

Each correct answer represents a complete solution. Choose three.

A. Security control monitoring

B. Status reporting and documentation

C. Configuration Management and Control

D. Network impact analysis

Correct Answer: ABC

Continuous monitoring in any system takes place after initial system security accreditation. It involves tracking changes to the information system that occur during its lifetime, and then determines the impact of those changes on the system security. Due to the necessary changes in hardware, software, and firmware during the lifetime of an information system, an evaluation of the results of these modifications has to be conducted to determine whether corresponding changes necessarily have to be made to security controls, to bring the system to the desired security state.

Continuous Monitoring is the fourth phase of the Security Certification and Accreditation process.

The Continuous Monitoring process involves the following three activities:

1.

Configuration Management and Control

2.

Security control monitoring and impact analysis of changes to the information system.

3.

Status reporting and documentation

1. Configuration management and control: This activity involves the following functions:

o Documentation of information system changes

o Security impact analysis

2. Security control monitoring: This activity involves the following functions:

o Security control selection

o Selected security control assessment

3. Status reporting and documentation: This activity involves the following functions:

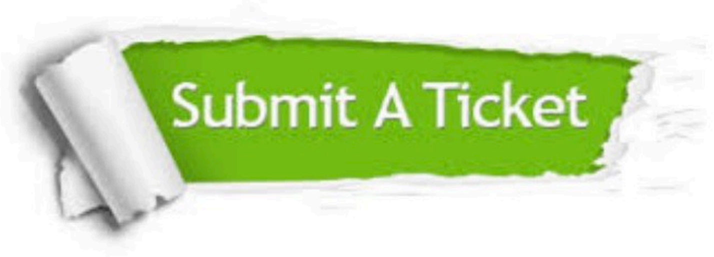
o System security plan update

o Plan of action and milestones update

o Status reporting

The objective of these tasks is to observe and evaluate the information system security controls during the system life cycle. These tasks determine whether the changes that have occurred will negatively impact the system security.

Answer option D is incorrect. It is not a valid activity.


Submit A Ticket