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.passapply.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 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.

Correct Answer: A

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.

QUESTION 2

Which of the following requires all general support systems and major applications to be fully certified and accredited before these systems and applications are put into production? Each correct answer represents a part of the solution. Choose all that apply.

A. NIST

B. Office of Management and Budget (OMB)

C. FIPS

D. FISMA

Correct Answer: BD

FISMA and Office of Management and Budget (OMB) require all general support systems and major applications to be fully certified and accredited before they are put into production. General support systems and major applications are also referred to as information systems and are required to be reaccredited every three years. Answer: A 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. Answer: C is incorrect. The Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States federal government for use by all non- military government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community (ANSI, IEEE, ISO, etc.). Some FIPS standards were originally developed by the U.S. government. For instance, standards for encoding data (e.g., country codes), but more significantly some encryption standards, such as the Data Encryption Standard (FIPS 46-3) and the Advanced Encryption Standard (FIPS 197). In 1994, NOAA (Noaa) began broadcasting coded signals called FIPS (Federal Information Processing System) codes along with their standard weather broadcasts from local stations. These codes identify the type of emergency and the specific geographic area (such as a county) affected by the emergency.

QUESTION 3

A service provider guarantees for end-to-end network traffic performance to a customer. Which of the following types of agreement is this?

A. SLA

B. VPN

C. NDA

D. LA

Correct Answer: A

This is a type of service-level agreement. A service-level agreement (SLA) is a negotiated agreement between two parties where one is the customer and the other is the service provider. It records a common understanding about services, priorities, responsibilities, guarantees, and warranties. Each area of service scope should have the \\'level of service\\' defined. The SLA may specify the levels of availability, serviceability, performance, operation, or other attributes of the service, such as billing. Answer: C is incorrect. Non-disclosure agreements (NDAs) are often used to protect the confidentiality of an invention as it is being evaluated by potential licensees. Answer: D is incorrect. License agreements (LA) describe the rights and responsibilities of a party related to the use and exploitation of intellectual property. Answer: B is incorrect. There is no such type of agreement as VPN.

QUESTION 4

Which of the following ISO standards is entitled as "Information technology - Security techniques - Information security management - Measurement"?

A. ISO 27003

B. ISO 27005

C. ISO 27004

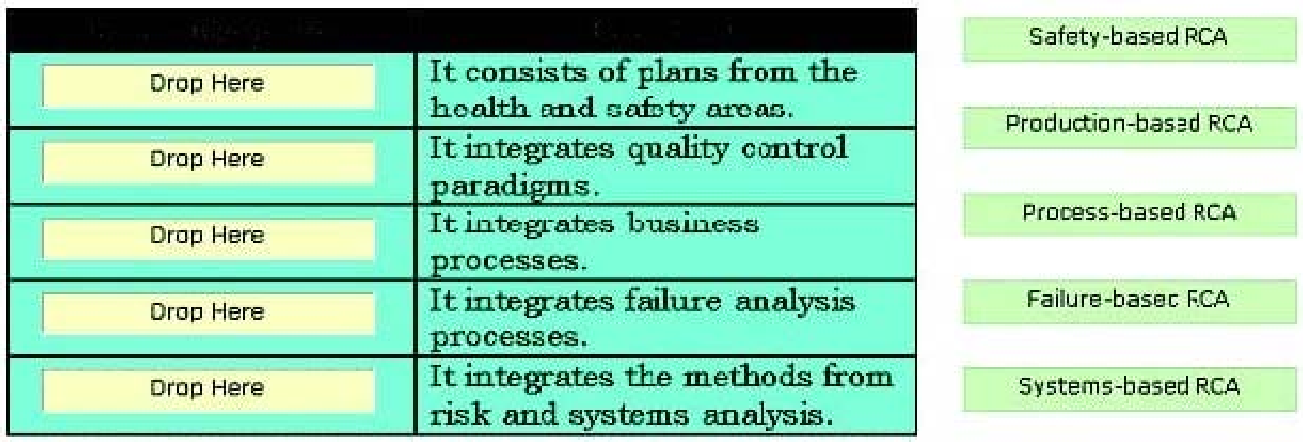
D. ISO 27006

Correct Answer: C

ISO 27004 is an information security standard developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is entitled as "Information technology - Security techniques Information security management - Measurement". The ISO 27004 standard provides guidelines on specifications and use of measurement techniques for the assessment of the effectiveness of an implemented information security management system and controls. It also helps an organization in establishing the effectiveness of ISMS implementation, embracing benchmarking, and performance targeting within the PDCA (plan-do-check-act) cycle. Answer: A is incorrect. ISO 27003 is entitled as "Information Technology - Security techniques - Information security management system implementation guidance". Answer: B is incorrect. ISO 27005 is entitled as "ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management". Answer: D is incorrect. ISO 27006 is entitled as "Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems".

QUESTION 5

RCA (root cause analysis) is an iterative and reactive method that identifies the root cause of various incidents, and the actions required to prevent these incidents from reoccurring. RCA is classified in various categories. Choose appropriate categories and drop them in front of their respective functions.



Drop Here	It consists of plans from the health and safety areas.
Drop Here	It integrates quality control paradigms.
Drop Here	It integrates business processes.
Drop Here	It integrates failure analysis processes.
Drop Here	It integrates the methods from risk and systems analysis.

Safety-based RCA

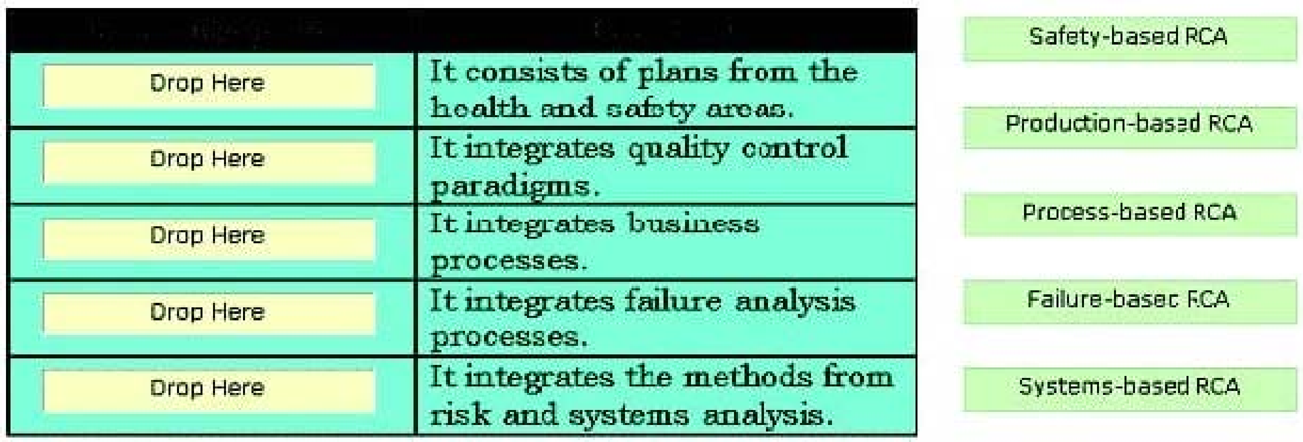
Production-based RCA

Process-based RCA

Failure-basec RCA

Systems-based RCA

Select and Place:



Drop Here	It consists of plans from the health and safety areas.
Drop Here	It integrates quality control paradigms.
Drop Here	It integrates business processes.
Drop Here	It integrates failure analysis processes.
Drop Here	It integrates the methods from risk and systems analysis.

Safety-based RCA

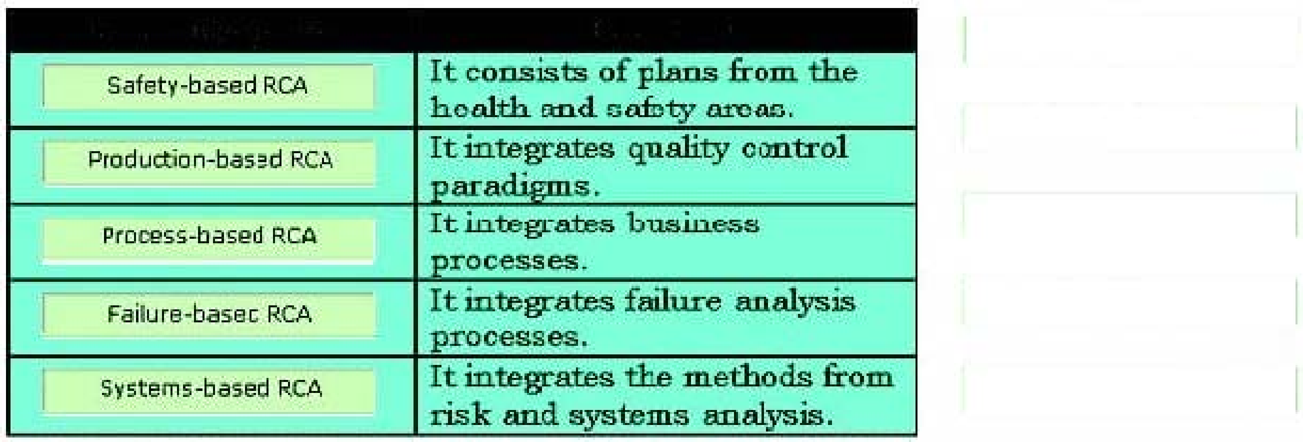
Production-based RCA

Process-based RCA

Failure-basec RCA

Systems-based RCA

Correct Answer:



Safety-based RCA	It consists of plans from the health and safety areas.
Production-based RCA	It integrates quality control paradigms.
Process-based RCA	It integrates business processes.
Failure-basec RCA	It integrates failure analysis processes.
Systems-based RCA	It integrates the methods from risk and systems analysis.

The various categories of root cause analysis (RCA) are as follows: Safety-based RC A. It consists of plans from the health and safety areas. Production-based RCA. It integrates quality control paradigms. Process-based RCA. It integrates business processes. Failure-based RCA. It integrates failure analysis processes as employed in engineering and maintenance. Systemsbased RCA. It integrates the methods from risk and systems analysis.