DUMPSARENA

Certified Secure Software Lifecycle Professional

ISC2 CSSLP

Version Demo

Total Demo Questions: 15

Total Premium Questions: 349

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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.

QUESTION NO: 2

You are the project manager for GHY Project and are working to create a risk response for a negative risk. You and the project team have identified the risk that the project may not complete on time, as required by the management, due to the creation of the user guide for the software you're creating. You have elected to hire an external writer in order to satisfy the requirements and to alleviate the risk event. What type of risk response have you elected to use in this instance?

A. Transference

B. Exploiting

C. Avoidance

D. Sharing

ANSWER: A

Explanation:

This is an example of transference as you have transferred the risk to a third party. Transference almost always is done with a negative risk event and it usually requires a contractual relationship.

QUESTION NO: 3

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

ANSWER: C

Explanation:

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 NO: 4

What component of the change management system is responsible for evaluating, testing, and documenting changes created to the project scope?

A. Project Management Information System

B. Integrated Change Control

C. Configuration Management System

D. Scope Verification

ANSWER: C

Explanation:

The change management system is comprised of several components that guide the change request through the process. When a change request is made that will affect the project scope. The Configuration Management System evaluates the change request and documents the features and functions of the change on the project scope.

QUESTION NO: 5

Which of the following is designed to detect unwanted attempts at accessing, manipulating, and disabling of computer systems through the Internet?

A. DAS

B. IPsec

C. IDS

D. ACL

ANSWER: A B C D

Explanation:

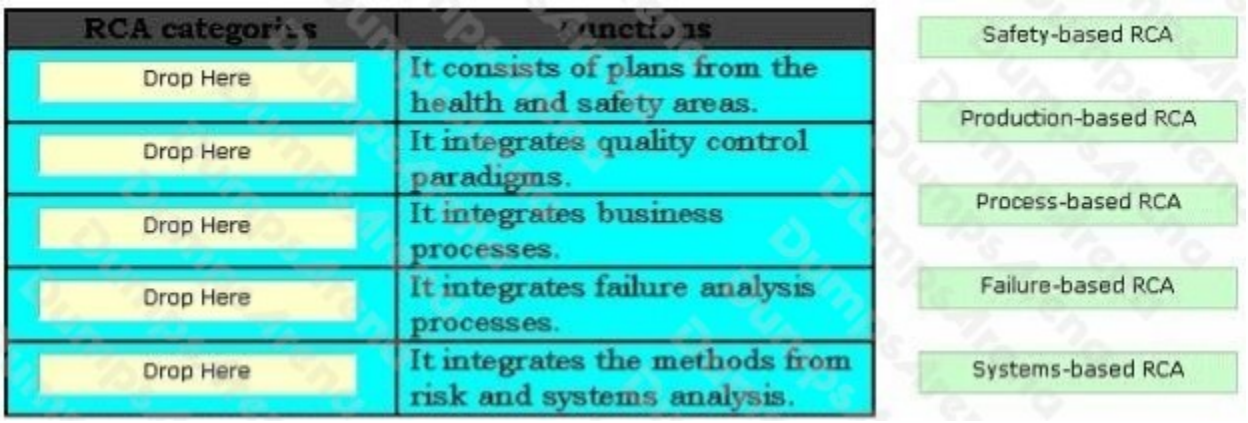
Answer: An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers, malware and/or disgruntled employees. An IDS cannot directly detect attacks within properly encrypted traffic. An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, trojan horses, and worms). D is incorrect. Access Control List (ACL) is the most commonly used object in Cisco IOS. It filters packets or network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. According to the criteria specified within the access lists, router determines whether the packets to be forwarded or dropped. Access control list criteria could be the source or destination address of the traffic or other information. The types of Cisco ACLs are Standard IP, Extended IP, IPX, Appletalk, etc. B is incorrect. Internet Protocol Security (IPSec) is a method of securing data. It secures traffic by using encryption and digital signing. It enhances the security of data as if an IPSec packet is captured, its contents cannot be read. IPSec also provides sender verification that ensures the certainty of the datagram's origin to the receiver. A is incorrect. Direct-attached storage (DAS) is a digital storage system that is directly attached to a server or workstation, without using a storage network.

QUESTION NO: 6 - (DRAG DROP)

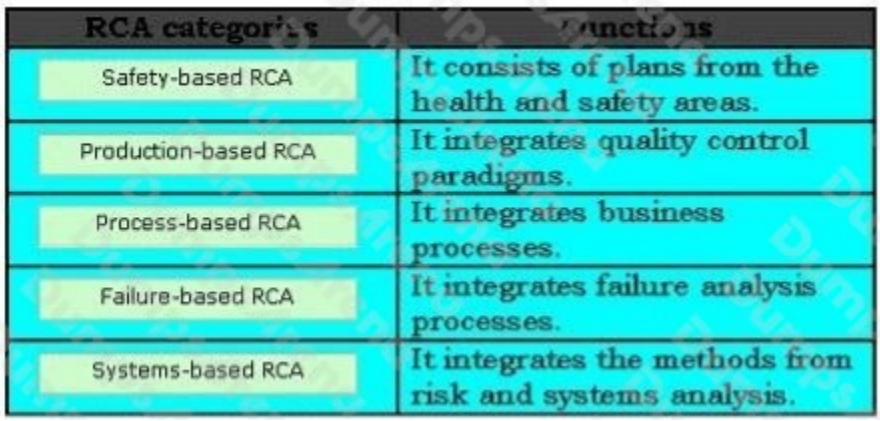
DRAG DROP

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.

Select and Place:



ANSWER:



RCA categories	Functions
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-based RCA	It integrates failure analysis processes.
Systems-based RCA	It integrates the methods from risk and systems analysis.

Explanation:

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. Systems-based RCA. It integrates the methods from risk and systems analysis.

QUESTION NO: 7

ISO 27003 is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Which of the following elements does this standard contain? Each correct answer represents a complete solution. Choose all that apply.

A. Inter-Organization Co-operation

B. Information Security Risk Treatment

C. CSFs (Critical success factors)

D. ystem requirements for certification bodies Managements

E. Terms and Definitions

F. Guidance on process approach

ANSWER: A B C D E F

Explanation:

Answer: ISO 27003 is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is entitled as "Information Technology - Security techniques Information security management system implementation guidance". The ISO 27003 standard provides guidelines for implementing an ISMS (Information Security Management System). It mainly focuses upon the PDCA method along with establishing, implementing, reviewing, and improving the ISMS itself. The ISO 27003 standard contains the following elements: Introduction Scope Terms and Definitions CSFs (Critical success factors)

Guidance on process approach Guidance on using PDCA Guidance on Plan Processes Guidance on Do Processes Guidance on Check Processes Guidance on Act Processes Inter-Organization Co-operation B is incorrect. This element is included in the ISO 27005 standard. D is incorrect. This element is included in the ISO 27006 standard.

QUESTION NO: 8

Which of the following NIST documents provides a guideline for identifying an information system as a National Security System?

A. NIST SP 800-37

B. NIST SP 800-59

C. NIST SP 800-53

D. NIST SP 800-60

E. NIST SP 800-53A

ANSWER: B

Explanation:

NIST has developed a suite of documents for conducting Certification & Accreditation (C&A). These documents are as follows: NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems. NIST Special Publication 800-53: This document provides a guideline for security controls for Federal Information Systems. NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System. NIST Special Publication 800-59: This document is a guideline for identifying an information system as a National Security System. NIST Special Publication 800-60: This document is a guide for mapping types of information and information systems to security objectives and risk levels.

QUESTION NO: 9

In which of the following deployment models of cloud is the cloud infrastructure administered by the organizations or a third party? Each correct answer represents a complete solution. Choose two.

A. Private cloud

B. Public cloud

C. Hybrid cloud

D. Community cloud

ANSWER: B C

Explanation:

Answer: In private cloud, the cloud infrastructure is operated exclusively for an organization. The private cloud infrastructure is administered by the organization or a third party, and exists on premise and off premise. In community cloud, the cloud infrastructure is shared by a number of organizations and supports a particular community. The community cloud infrastructure is administered by the organizations or a third party and exists on premise or off premise. B is incorrect. In public cloud, the cloud infrastructure is administered by an organization that sells cloud services. C is incorrect. In hybrid cloud, the cloud infrastructure is administered by both, i.e., an organization and a third party.

QUESTION NO: 10

Which of the following rated systems of the Orange book has mandatory protection of the TCB?

A. A-rated

B. B-rated

C. D-rated

D. C-rated

ANSWER: B

Explanation:

A B-rated system of the orange book has mandatory protection of the trusted computing base (TCB).

Trusted computing base (TCB) refers to hardware, software, controls, and processes that cause a computer system or network to be devoid of malicious software or hardware. Maintaining the trusted computing base (TCB) is essential for security policy to be implemented successfully.

QUESTION NO: 11

Which of the following SDLC phases consists of the given security controls: Misuse Case Modeling Security Design and Architecture Review Threat and Risk Modeling Security Requirements and Test Cases Generation?

A. Deployment

B. Requirements Gathering

C. Maintenance

D. Design

ANSWER: D

Explanation:

The various security controls in the SDLC design phase are as follows:

Misuse Case Modeling: It is important that the inverse of the misuse cases be modeled to understand and address the security aspects of the software. The requirements traceability matrix can be used to track the misuse cases to the functionality of the software. Security Design and Architecture Review: This control can be introduced when the teams are engaged in the "functional" design and architecture review of the software. Threat and Risk Modeling: Threat modeling determines the attack surface of the software by examining its functionality for trust boundaries, data flow, entry points, and exit points. Risk modeling is performed by ranking the threats as they pertain to the users organization's business objectives, compliance and regulatory requirements and security exposures. Security Requirements and Test Cases Generation: All the above three security controls, i.e., Misuse Case Modeling, Security Design and Architecture Review, and Threat and Risk Modeling are used to produce the security requirements.

QUESTION NO: 12 - (SIMULATION)

SIMULATION

Fill in the blank with an appropriate security type. applies the internal security policies of the software applications when they are deployed.

ANSWER: Programmatic security

Explanation:

Programmatic security applies the internal security policies of the software applications when they are deployed. In this type of security, the code of the software application controls the security behavior, and authentication decisions are made based on the business logic, such as the user role or the task performed by the user in a specific security context.

QUESTION NO: 13

Which of the following is generally used in packages in order to determine the package or product tampering?

A. Tamper resistance

B. Tamper evident

C. Tamper data

D. Tamper proof

ANSWER: B C D

Explanation:

Answer: Tamper resistance is resistance tampered by the users of a product, package, or system, or the users who can physically access it. It includes simple as well as complex devices. The complex device encrypts all the information between individual chips, or renders itself inoperable. Tamper resistance is generally used in packages in order to determine package or product tampering. B is incorrect. Tamper evident specifies a process or device that makes unauthorized access to the protected object easily detected. D is incorrect. Tamper proofing makes computers resistant to interference. Tamper proofing measures include automatic removal of sensitive information, automatic shutdown, and automatic

physical locking. C is incorrect. Tamper data is used to view and modify the HTTP or HTTPS headers and post parameters.

QUESTION NO: 14

Which of the following terms refers to the protection of data against unauthorized access?

A. Integrity

B. Recovery

C. Auditing

D. Confidentiality

ANSWER: A B C D

Explanation:

Answer: Confidentiality is a term that refers to the protection of data against unauthorized access. Administrators can provide confidentiality by encrypting data. Symmetric encryption is a relatively fast encryption method. Hence, this method of encryption is best suited for encrypting large amounts of data such as files on a computer. A is incorrect. Integrity ensures that no intentional or unintentional unauthorized modification is made to data. C is incorrect. Auditing is used to track user accounts for file and object access, logon attempts, system shutdown etc. This enhances the security of the network. Before enabling auditing, the type of event to be audited should be specified in the Audit Policy in User Manager for Domains.

QUESTION NO: 15

"Enhancing the Development Life Cycle to Produce Secure Software" summarizes the tools and practices that are helpful in producing secure software. What are these tools and practices? Each correct answer represents a complete solution. Choose three.

A. Leverage attack patterns

B. Compiler security checking and enforcement

C. Tools to detect memory violations

D. Safe software libraries

E. Code for reuse and maintainability

ANSWER: A C D E

Explanation:

Answer: The tools and practices that are helpful in producing secure software are summarized in the report "Enhancing the Development Life Cycle to Produce Secure Software". The tools and practices are as follows: Compiler security checking and enforcement Safe software libraries Runtime error checking and safety enforcement Tools to detect memory violations Code obfuscation A and E are incorrect. These are secure coding principles and practices of defensive coding.